ISSN : 0974 - 7435 Volume 10 Issue 23

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(23), 2014 [14752-14756]

Research and implementation of security protocols technology based on trusted computing platform

Chen Ya-dong[1,2], Sun Zhi-xin[1], Zhang Tao[1,2]
[1]Nanjing University of Posts and Telecommunications, 210003, (CHINA)
[2]China Electric Power Research Institute, 210003, (CHINA)

ABSTRACT

With the rapid development of Internet, the security issues faced by computer system and computer network are more and more serious. Security protocol is a research hotspot in current network security filed and plays an important role in protecting network security. But if the information is replaced by viruses, Trojans, or tampered before encryption, the transmittal information has alreadyfailed although protocol itself is safe.

Trusted computing platform only run the program of trusted source guarantee, and ensure the running program is legal. At the same time, the platform can stop the virus and malicious code running, the trusted computing platform solve the problem of the security of the encryption system and its running environment.

If the current security protocol without modified directly to use on the trusted computing platform, although it can guarantee the communication security but do not play the advantage of the trusted computing platform, protocol execution efficiency is not high, and also unable to complete the authentication of platform.

Based on the status research of trusted computing platform and security protocol, and aiming at the shortcomings of the current security protocol, this paper puts forward the safety communication protocol based on trusted computing platform. At the same time, using the formal method verifies protocol, and writes the middle tier of the NDIS driver implement the protocol.

Security protocols running on the safe and reliable platform, achieve real efficient and secure communication. In the research process, the research mainly achieved the following research results:

1. Establish security protocol model based on trusted computing platform.

2.In the process of analyzing the protocol, theoretically prove protocol security, not only use attack validation but also use the formal analysis.

Compared to the traditional security protocol, the protocoldesigned and implemented in this paper applies on the trusted computing platform, data computing speed is faster, protocol execution efficiency is higher,information transmission is more security.

KEYWORDS

Trusted computing platform; Identity authentication; Security protocols; Formal verification.

© Trade Science Inc.

THE ANALYSIS AND RESEARCH OF THE TNC SPECIFICATIONS

Facing multiple forms of cyber attacks: viruses, network worms, Trojan horses, etc., the original user authentication in network protocol cannot guarantee the reliability of the network connection. Therefore, TCG (Trusted Computing Group) commits to the research of Trusted Computing and introduces a new safety machine control technology, such as: platform attestation and terminal completive validation, and publishes TNC (Trusted Network Connection) specification in May 2005, and has established an enhanced and reliability of the Network security architecture.

TNC structure

TNC is from IWG structure extension, Figure 1 is the contrast figure of TNC institutions and IWG structure, AR is access requestor, PDP is policydecision point, PEP is policy enforcementpoint[1].

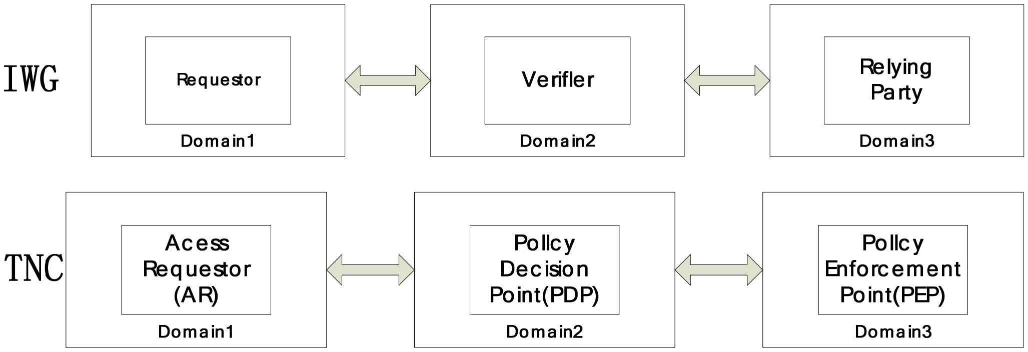

Figure 1 : TNC structure and IWG structure contrast diagram

In IWG structure,Requestor sends request, Relying Party responses to request is decided by Verifier, this model behavior corresponds to the behavior of the network connection, so in TNC architecture, AR is equivalent to the Requestor, TNC PDP is equivalent to IWG Verifier, TNC PEP is equivalent to the IWG Relying Party. Figure 2 is TNC structure, which includes a variety of network equipments, network topology and configuration.

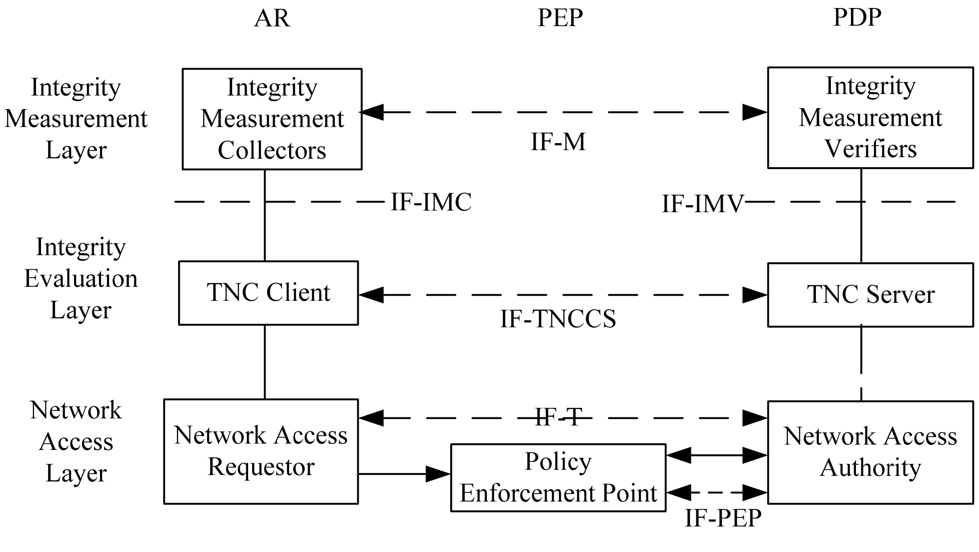

Figure 2 : TNC structure

TNC structure is divided into three layers: network access layer, integrity evaluation layer and integrity measurement layer. Network access layer contains NAR (Network Access Requestor), PEP (Policy Enforcement Point) and NAA (Network Access Authority); Integrity evaluation layer contains TNC Client and TNC Server; Integrity measurement layer contains Integrity Measurement Collectors and Integrity Measurement Verifiers.

TNC structure has several interface, they have defined the relationship between the components of TNC structure:

1)IF-IMC interface

IF - IMC is the direct interface of integrity measurement terminal and TNC Clint. IF- IMC mainly collects data from the integrity measurement terminal, and transfers the data to integrity verifier terminal, responsible for the communication between integrity measurement terminal and integrity verifier terminal.

2)IF-IMV interface

IF - IMV is the interface of integrity verifier terminal and TNC server. IF - IMV mainly receive the integrity data send by TNC Client, which is responsible for the communication between integrity measurement terminal and integrity verifier terminal, and send the integrity verifier response to the TNC Client.

3) IF-TNCCS interface

IF-TNCCS is the direct interface of TNC client and TNC server, and responsible for the data communication between TNC Clint and TNC server. It mainly transfer three types of data: the data of integrity measurement to integrity Verifier, the data of integrity Verifier to integrity measurement and the synchronous coordinate data between TNC client and TNC server.

4) IF-M message

IF-M is the specific information between integrity measurement and integrity verifier. In practice, these messages are interacted through IF-TNCCSS interface.

5) IF-T protocol

IF-T is the message transfer protocol between network access requestor and policy decision point, is responsible for the message transmission between network access requestor and the network access authentication center.

6) IF-PTS interface

IF-PTS interfaces provide platform trusted service, the interface is not yet standardized.

7) IF-PEP interface is responsible for the communication between the policy decision point and policy enforcement point

TNC message structure

There are a lot of message interacted through interfaces in the TNC structure, message flow and process sequence as shown in Figure 3:

Flow 0: Before the network connection checking the integrity, TNC Client must find each integrity measurement, and initialize it.

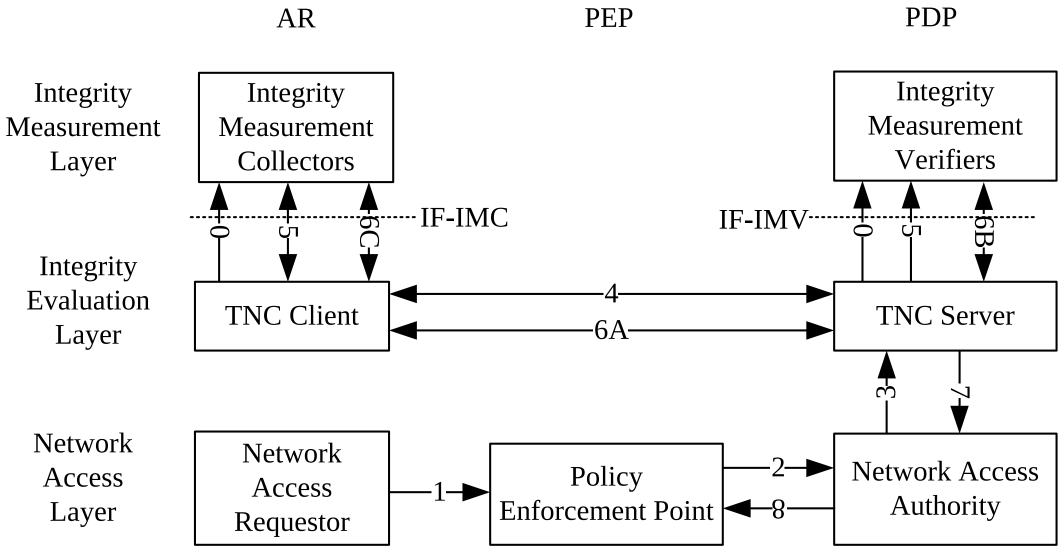

Figure 3 : Flow chart of TNC message structure

Flow1: When trigger one connection request, NAR began to initiate a connection requests in the network layer.

Flow2: After PEP receiving the connection request from the NAR, PEP sends a network access license request to NAA. NAA must accord with the order of user authentication, platform authentication and integrity check.

Flow3: The user through authentication, NAA send network connection requests to TNC Server.

Flow4: After TNC Server receiving the network connection requests, began to platform certification to TNC Client.

Flow5: After platform certification between TNC Server and TNC Client, TNC Server inform IMVs that there is a new type network connection request needs integrity check handshake requests; Similarity, TNC Client inform IMCS that there is a new type network connection request and receive an integrity check handshake request in TNC Client.

Flow6A：Do integrity check handshake between TNC Server and TNC Client.

Flow6B: In TNC Server, the message from integrity verifiers sends to integrity verifiers.

Flow6C: In TNC Server, the message from integrity verifiers sends to integrity measurement.

Flow7: After finishing the integrity check handshake between with TNC Client in TNC Server, send suggestions to NAA.

Flow8: NAA sends network access license decision to PEP.

TNC structure can through auditing terminal integrity and setting up the safety rules to enhance security and prevent the network attack before network connect is established. Compared to previous security model, TNC provides a new anti-attack strategy, namely the terminal integrity detection and platform verification. Through the terminal integrity detection and platform verification can solve the problem of the client's own security. Prevent Trojan horse attack[2].

SECURITY COMMUNICATION PROTOCOL BASED ON TRUSTED COMPUTING PLATFORM

Protocol description

Protocol includes the client A, server B and the trusted third party CA. A and B each has its own private key and public key (set to, and,), and have the credential certificated by CA (set to CertA and CertB, register claims by artificial to CA centerbefore using of trusted computing platform). A and B are all use trusted computing platform, TPM chip complete the encryption and signature verification, before A implement protocol link CA to download B certificates to get B public key.

The security analysis of the protocol

(1) The confidentiality of the message

Protocol is based on the trusted computing platform, thus it can be prevent the information need to encrypt replacing by Trojans or tampered before encryption, and ensure that don’t appear plaintext in the whole process of message transmission.

(2)The integrity of the message

The protocol uses Hash algorithm to calculate the text messages, and then encrypt the Hash value to complete the signature. In the second step, A verified B signature to confirm whether message from B, and can determine whether the message was modified at the same time. Because if the message is inserted, tampering or remake, the hash values will change, in the third step, B verify A signature, so A and B is verified each other[4].

(3)Non-repudiation

Non-repudiation is mainly aimed at A, because in the actual application A is the client network requestor, B is network server provide service. Through the protocol can protect the A client login to the service B doing malicious operation denied that landed on the service B, just keep A signature file in B {T + 1} :, at the same time A retain B signature file {{K、T},}can also prevent denial of B.

(4)Prevent the closure forwarding attacks

The protocol has been added symmetric keyK of A and B communication in the second step to prevent the closureforwarding attacks.

(5)Prevent reply attack

The time stamp T can prevent replay attack[5].

(6)Performance analysis

The protocol is based on trusted computing platform, the private key in card not only has high security, and makes the private key can have a longer lifespan and avoids apply for the certificate of operation to CA because of frequent changes the key. Compared with the previous security communication protocol, the protocol ensures key security while reducing the number of operations.

In the past security protocol, the sender or the receiver always send messages to CA, CA do the authentication and signature, then send the signed message to the receiver or sender by the CA[6]. The CA calculation is very large when the message need to send is large, CA has become the bottleneck of the whole communication system[7]; The trusted third party CA has rarelyreceiving and processing data in the protocol, and don't need to send A or B message do authentication and signature operation, break through the bottleneck of the whole communication system, not only guarantee the communication security but also greatly improve the efficiency of the communication. After B receive A connection request don't have to download A certificate to obtain the public key from CA, so that the server can response several clients connection and improve the working efficiency.

The securecommunication protocol based on computing Platform solves the ID card, data confidentiality and integrity, and non-repudiation of both communication sides. Due to the protocol is based on the trusted computing platform, thus ensure he authenticity and security of pass messages.

EXPERIMENTAL ANALYSIS

On the basis of the trusted computing technology, further propose a high trusted computerbased on the security control module (HT CBSCM) architecture, the experimental data are mainly associated with HT CBSCM integrity measurement of performance test data, namely the hash operation speed, as shown in Figure 5.

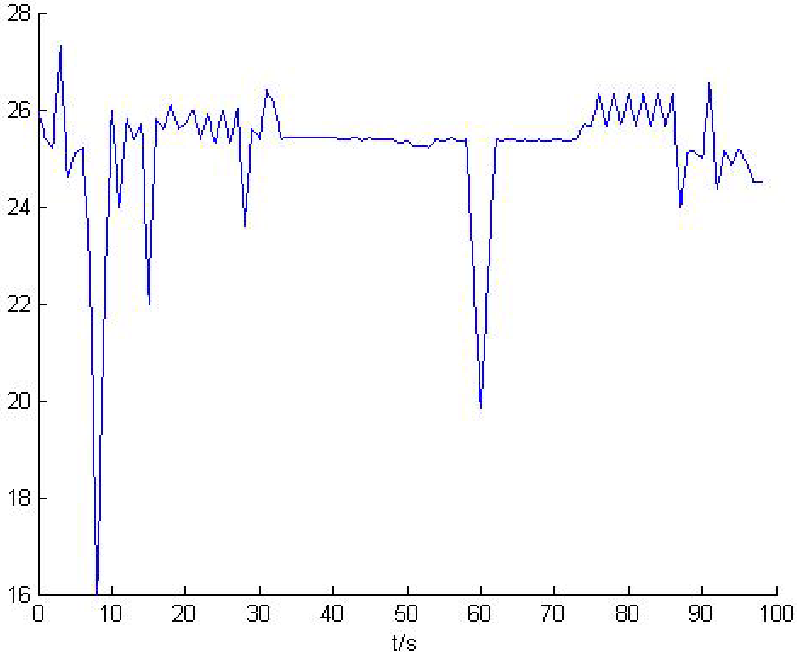

Figure 5 : Hash compute speed test

Result analysis

HTCBSCM function experiment is based on the system levelblack-box testing method, through the test, it can correctly implement the main safety function scheduled (trusted BIOS integrity measurement, key hardware equipment integrity measurement, software component integrity measurement, user authentication). In terms of performance, from test data of the hash speed in Figure 4 can obtainthat HT CBSCM average speed of hash computing is about 27 MB/s. Considering the main steps in startup process of the system of hash algorithm, and combining with related data bus transmission time, can calculate the time loss theoretical value in HT CBSCM trust chain transmission.

(1) Hash compute time: T=T BIOS+TKH+TKS, T BIOS,TKH and TKSrespectively represent for credible BIOS (512 KB), key hardware device (16 KB) and software components (13 MB) operation time.

(2) Bus transmission time: T = TLPC+T PC I, TLPC, TPC, I respectively represent for IBIOS, other data need to measure in LPC bus (33 MHz, bit 4 bits) and PCI bus (33 MHz, 32 bits) transmission time. From the above analysis can calculate the loss time theoretical value is 1.9 s. The value has certain deviation with the measured values 4.4s of performance tester testing, this is due to not consider the resolution time, of measurement data, USBKey communication time and CPU running time. Overall, HTCB-SCM integrity measurement process performance influence is relatively small to the system.

REFERENCES

[1] Guan Zhensheng; The public key infrastructure PKI and CA certification institutions, Beijing: Electronic industry press, **(2008)**.

[2] Wu Shizhong, ZhuShiXiong, Zhang Wenzheng; Interpret, Applied cryptography: Protocols, Algorithms and C source program, Machinery industry press, **(2010)**.

[3] Nancy R.Mead; McGraw understanding trusted computing will its benefits outweigh its drawbacks, Iees Security & Privacy, May/June, **(2012)**.

[4] Wang Yayong, Li Daxing; PKI research progress and applications, Communication confidentiality protocol, **3**, **(2010)**.

[5] Li Zhenglin, Hao Shuwei; Yu Shiquan is a secure email protocol design based on PKI, Microcomputer development, **13**, 7 **(2009)**.

[6] G.Lowe; Breaking and fixing then needham-schroeder public-key protocol using FDR, In CSFW-11 IEEE Computer Society Press, **(2011)**.

[7] OMG; Public key infranstructure specification version 1.0.RFC, 2731 **(2011)**.

[8] Bill Arbaugh; Improving the TCPA Specification, Security, August, **(2012)**.