Realization of key technology of Trusted Network Connect based on IF-MAP protocol

Zelong Wang, Guoyang Cai, Wanzhen Liu
School of Information Science & Technology
Sun Yat-sen University
Guangzhou, China
isscgy@mail.sysu.edu.cn

***Abstract*—Network security has attracted increasing research interest in recent years. Through detailed investigations of the related structure of Trusted Network Connect (TNC), in this paper we research into the norms and key technology of Interface for Metadata Access Point (IF-MAP) protocol, as well as design and realize a prototype system of TNC based on the very protocol. The system includes trusted access module for endpoint computer and a security component that applies IF-MAP protocol. It realizes the sharing and interaction of security event information between firewall and Intrusion Detection System (IDS) and provides the capabilities of behavior determination for the endpoint computers and dynamic policy modification for firewalls.**

Keywords—Trusted Computing; Trusted Network Connect; Network Access Control; Metadata Access Point; Network Security

I. INTRODUCTION

Computer networks have brought tremendous convenience to people's life, however, many network security problems exist, such as those caused by virus and Trojan. Those problems pose great security challenges to people's life. In order to resolve the problems, the following measures are usually taken for ensuring network security: anti-virus software, firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) [1]. However, those measures fail to prevent the computer system infected by malwares from malicious behaviors on internet [2].

In light of the abovementioned challenges, trusted computing, as a novel solution scheme, has attracted great attention. Trusted Network Connect (TNC) norms formulated by Trusted Network Connect Sub Group (TNC-SG) are essential to establish network connection with security and trust based on terminal integrity. Based on traditional network access authentication, TNC requires more functions including identity authentication and integrity verification of platform. The terminal computers are allowed to access network after successful identification of terminal user and its integrity verification.

To manage trusted network state after accessing the network by terminal user, TNC-SG introduces IF-MAP protocol into the new TNC framework. IF-MAP protocol provides a method of presenting metadata of network security event and defines the mechanism of security event set. It can realize information sharing of security event and the dynamic management of security policy. By introducing an IF-MAP protocol, TNC framework establishes data model, data operation and communication mode to perform information sharing and interaction between necessary components of TNC (such as Policy Decision Point and Policy Enforcement Point) and traditional network security device (such as firewall, or IDS). Various security devices realize information sharing of network security event. The information not only reflects security state of network terminal, but also facilitates the security devices to realize dynamic management of security policies in view of the policies of network access control.

Section 2 in this paper introduces TNC frameworks including basic framework and the IF-MAP protocol framework; in Section 3 we demonstrate a TNC scheme based on IF-MAP, each main module in framework is analyzed and introduced; Concluding remarks are given in Section 4.

II. TNC BASED ON IF-MAP

A. Basic Framework of TNC

Trusted computing platform applies trusted platform module (TPM) chip for trusted root to establish the trust computing chain inside a terminal system. In addition, the trusted computing platform is capable of expanding the trust chain into network by ensuring terminal dependability, namely building the trusted network. To build trusted network, a set of policies for expressing the internal system status in trusted network needs to be established. In such circumstances, a terminal computer can access the network only if the terminal policies are followed. Devices not following the policies will be located and isolated. The policies are shown as follows: installing and accurately collocating latest anti-virus software, frequently running virus scanning, precisely running and collocating personal firewall, installing latest patch of operating system and forbidding running unauthorized software, etc. TNC framework presents double standards including integrity and authentication. Its open standard provides supports for collecting and exchanging integrity data of terminal computer under various network environments, and is compatible with standard devices of TNC from different manufacturers so that it provides users with great conveniences.

The open design standard adopted by TNC includes three logical entities and three layers [3] as shown in Figure 1.

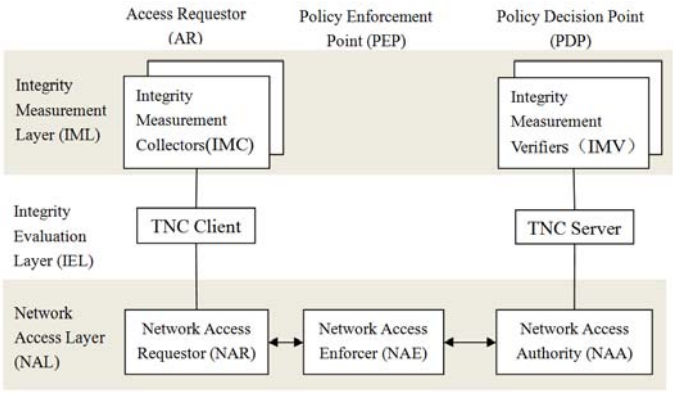

Fig. 1. Basic framework of TNC

TNC framework consists of three logical entities as follows:

- Access Requestor (AR) is responsible for running terminal device of TNC client and sending request of access network. After being allowed to access the network, it is able to conduct various operations in network.
- Policy Enforcement Point (PEP) connects AR directly, performs the practical operations of permitting or prohibiting access requests initiated by Policy Decision Point (PDP), and physically acts as the switch.
- PDP is to decide whether AR can be allowed to access network or not according to network access control policy and AR access requests.

TPM is considered as the basis of operating system trust. Remote attestation technology and integral report protocol supported by TPM chip can transfer the trust of TPM to network. TNC expands the application of trusted computer platform and combines trusted computing technology with network access control. Before terminal accesses network, it verifies the integrity and state of platform to decide terminal's state through user authentication.

B. TNC Framework Extended by IF-MAP Protocol

1) The necessity of IF-MAP protocol

The basic TNC framework includes terminal access, AAA platform, and network access device and policy management platform. It initially constructs a prevention system for controlling terminal access to network, but it does not integrate the security detection devices (such as IDS) and security protection devices (such as firewall and Flow Controller). The information between TNC and traditional network security technology cannot be shared and exchanged, which results in information isolation among various security devices, increasing the difficulty in protecting network security. To solve the problem, TNC-SG extends TNC framework by introducing IF-MAP protocol is designed for presenting and exchanging security information. It defines the formats and communication modes of data with needs among network devices. Manufacturers realize data interaction of various devices by producing network devices supported by IF-MAP protocol norms, and achieves cooperation of various security devices on the basis.

2) IF-MAP protocol components

The extended TNC framework [4] is shown in Figure 2, with two newly entities, MAP and MAPC.

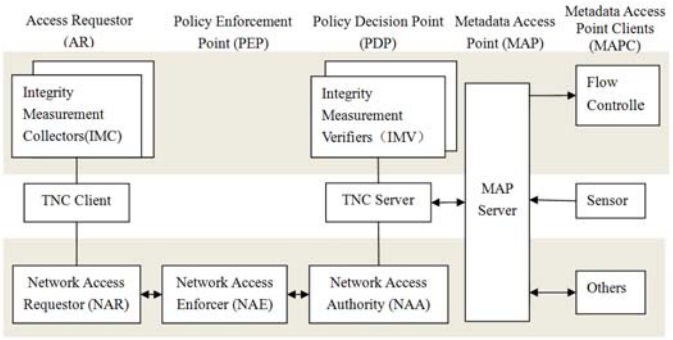

Fig. 2. TNC framework of extended IF-MAC

- Metadata Access Point (MAP) refers to a dependent MAP server which is used for concentrating various security attributes, security policies and security event information of trusted terminal in storage network so as to build an exchange platform of network security data.
- Metadata Access Point Clients (MAPC) include flow controller and sensor etc. and are realized by firewall and IDS. Traditional network security devices (such as IDS and firewall) can realize publishing and acquisition of security event information, and dynamically adjust network access control policies according to metadata state of network security of MAP server through the network security metadata.

IF-MAP is a protocol expressing the data and communication around MAP and its clients. After introducing IF-MAP protocol, TNC framework builds data model, data operation and communication mode to perform information sharing and interaction between necessary components of TNC (such as PDP and PEP) and traditional network security devices (such as firewall and IDS).

III. M-TNC: AN IF-MAP BASED SOLUTION SCHEME

In this paper, M-TNC, as a TNC prototype system, combines trusted terminal access technology with IF-MAP protocol. It shows advantages of network access control brought by IF-MAP protocol. Some of the requirements of security hypotheses in the prototype system are as following: each terminal computer in local area network (LAN) ships with a TPM chip. And the LAN environment, as a protected and trusted LAN, accepts access network request from terminal computer.

The terminal computers need to provide a request of trusted terminal access before accessing network, and are allowed to access network after permitted by the PDP security policy. The terminal with network access needs to be permitted by firewall in the case of accessing network resource. Firewall decides whether to permit or prohibit access according to the security event metadata stored on MAP server. Meanwhile the network behaviors of terminal computers in network are monitored by IDS; once IDS finds an illegal act, MAP server will receive its

corresponding security event and inform firewall to modify the corresponding access control policy of terminal computer.

A. Protocol Prototype Framework Design of M-TNC

Prototype framework of M-TNC is shown as in Figure 3. It integrates IF-MAP protocol to TNC based on IEEE 802.1X network access protocol which includes hardware layer, network layer, software layer, deployment layer and security target layer.

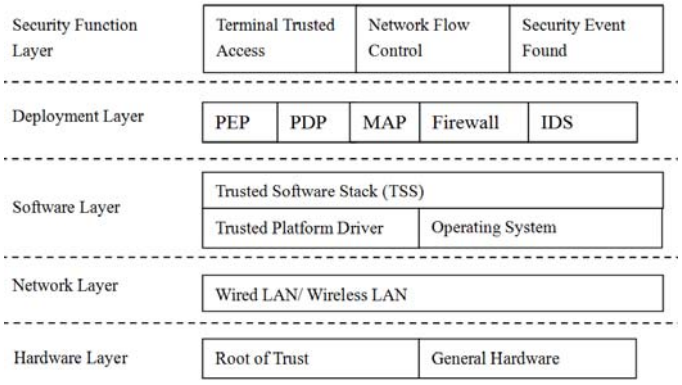

Fig. 3. Prototype system design of M-TNC

Hardware layer points out necessary hardware devices in M-TNC. Apart from conventional hardware devices, the root of trust, using the TPM chip shipped with PC motherboard, is needed.

Network layer points out the network environment of M-TNC. Both wired LAN and wireless LAN support IEEE 802.1X protocol so that they can both achieve the goal of network access control.

Software layer emphasizes the dependent software in M-TNC, including the TPM driver, the operating system which supports trusted computing, and the APIs provided by trusted software stack (TSS).

Deployment layer specifies all the functional components mentioned in M-TNC design, which include PEP, PDP, Network Security MAP, firewalls and IDS. These components constitute M-TNC together, achieving security goal of M-TNC.

Security target layer describes the security goals of M-TNC, including trusted network access of terminal computers, security event detection of network and the control of network flow.

The specific modules of M-TNC include trusted terminal interface module, PDP report module, network flow control module, and security event metadata management module. Figure 4 shows the locations of the abovementioned modules in TNC framework and standard components of various modules cooperation.

Referring to figure 4, the functions of each module are shown as follows:

- The network access terminal is running a secure operating system based on trusted computing technology. It gets access permission using remote attestation.
- PDP permits AR to access the network after the authentication. Afterward, the PDP report module publishes the news to the metadata management module.
- PEP opens the port in 802.1X so that AR accesses the protected network.
- The network flow control module cooperates with flow controller, controlling the access limits of network data after network accession of AR. Meanwhile, it communicates with metadata management module and updates the access control policy according to network events.
- The metadata management module records information about IP address, which bind with network events so that it is able to represent events such as logging in, exiting, data server accession, etc.
- The security event detection module cooperates with IDS, which monitors malicious behavior. When a malicious event is detected (for example, a port is being scanned), the security event detection module will publish AR's IP address and the event to the metadata management module. After that, the metadata management module updates the policy of this IP address (to block or to allow the access).

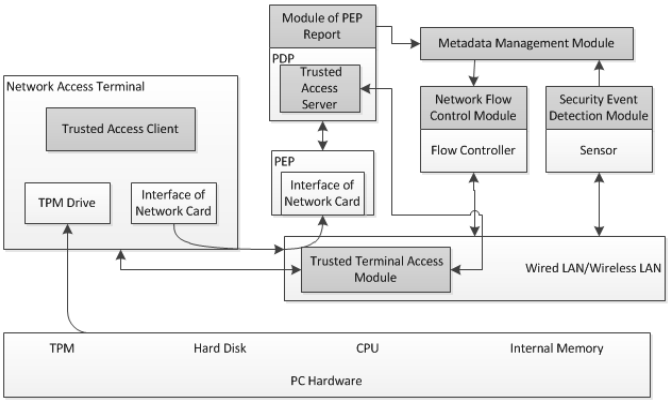

Fig. 4. The division and location of function module

B. The Design of Key Modules

Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".

1) Design of metadata management module

Metadata management module, as MAP server, takes charge of storing network event and communicating with other modules. For MAP client of executing metadata publish, metadata management module keeps monitoring the data published by client. While for the clients of subscribing and polling metadata, metadata management module executes subscription and records corresponding subscription information as client initializes; afterwards, management

module sends the modified metadata to client in polling process.

2) Design of PDP report module

When terminal accesses the network, PDP report module constructs metadata and execute publish operations. Based on the allocated terminal IP address, the format of the publishing data is <identity, ip, event>. IP and IF-MAP are the identifications ruled by IF-MAP protocol and the event refers to the metadata ruled by IF-MAP protocol. Functions of this module are as shown below:

- Communicate with metadata management module.
- Monitor login information of PDP user.
- Construct metadata of user login.
- Execute publishing operation.

Flow control of the module is shown in Figure 5; the constructed event information is regarded as the type of terminal behavior change based on the definition of IF-MAP and is published to metadata management module.

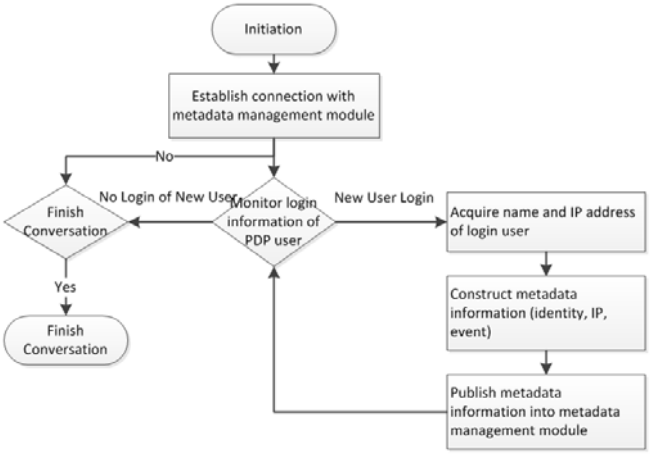

Fig. 5. Flow design of PDP report module

3) Design of network flow control module

When the terminal with network access needs to access data server, it is required to decide whether it is allowed to access or not according to the firewall's policy. Network flow control module is designed based on traditional firewall with the functions as following:

- Communicate with metadata management module to build SSRC and ARC.
- Use SSRC to subscribe metadata to metadata management module based on IP address of access.
- Use ARC to acquire update information of metadata to metadata management module
- Update information according to metadata and modify the current firewall policy
- Execute permission or prohibition function of terminal access.

4) Design of security event detection module

Security event detection module cooperates with IDS; when IDS detects illegal network behavior, security event metadata are produced and then published to metadata management module. Flow control of the module is shown in Figure 6. The functions are as following:

- Establish connection with metadata management module using the operations of publishing and notifying.
- Cooperate with IDS to detect network behavior.
- Classify the detected network behaviors.
- Metadata are constructed when there are some dangerous behaviors. After that, the data will be published to metadata management module. The data format is <ip, event>.

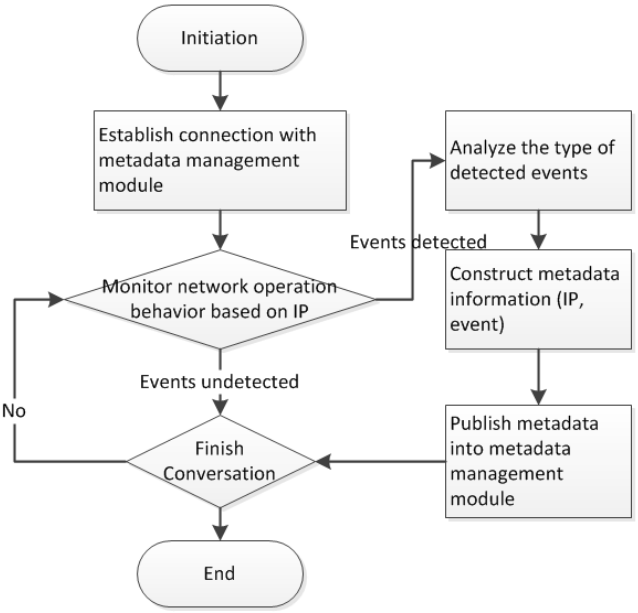

Fig. 6. Flow design of security event found module

IF-MAP network security norms define every kind of events as below:

- P2P: P2P application flow is detected;
- CVE: vulnerability defined by CVE is detected;
- Botnet infection: the terminal computer is infected by the botnet;
- Worm infection: the terminal computer is infected by the worm;
- Excessive flows: abnormal network flow is detected;
- Behavioral change: the behavior of terminal network has changed;
- Policy violation: the terminal violates the security policy;
- Other: other custom events.

C. Comparison and Analysis of Similar Products

Major network access control technology in the industry includes Trusted Network Connect (TNC), Cisco Network Admission Control (C-NAC) and Microsoft Network Access Protection (NAP). They are similar in 2 aspects: (1) they not only authenticate users, but also judge whether the terminal meets the network security policy or not; (2) they all use a ternary structure: the policy decision point, network access control device and the terminal computer. They have different priorities: C-NAC is designed around the Cisco network devices and it underlines the devices that are willing to access network. NAP is able to monitor the state of the terminal but it is limited to the windows operating system. TNC stresses "trusted" by binding the TPM chip with the terminal computer so that trusted state could be extended to the protected network.

M-TNC inherits the technical superiority of TNC, combining with firewalls and IDS. Using IF-MAP protocol to present and share metadata of network security, M-TNC integrate firewalls, IDS and PDP. Sharing network security data between devices, M-TNC proposes the solution of network access control. M-TNC does not depend on Microsoft operating system or Cisco network devices. Instead, M-TNC is compatible with existing devices and network norm. Therefore, M-TNC is more secure and reliable, possessing stronger compatibility and more developmental potential.

IV. CONCLUSION

This paper proposes a method for building a reasonable and active defense scheme of trusted network connection with the support of TPM chip using IF-MAP protocol. It is of theoretical and practical significance. TNC framework based on IF-MAP can ensure the security of terminal computer access using trusted computing technology; meanwhile it can realize the sharing and interaction of security event information from various security devices, thus the validity of network access control function is largely improved.

REFERENCES

[1] Anan Luo, Chuang Lin, Yuanzhuo Wang et al., "Security Quantifying Method and Enhanced Mechanisms of TNC," Chinese Journal of Computers. 2009, 32(5):887-898.

[2] Changxiang Shen, "Construct Prevention System of Active and Comprehensive Defense," Information Security and Communications Privacy, 2004(5):17-18.

[3] Trusted Computing Group, "Trusted Network Connect: TNC architecture for interoperability specification, version 1.3 [EB/OL]," https://www.trustedcomputinggroup.org, October 2008.

[4] Trusted Computing Group, "TNC IF-MAP Metadata for Network Security[EB/OL]," http://www.trustedcomputinggroup.org/files/resource_files/281C050E-1A4B-B294-D018131B07BC2030/TNC_IFMAP_Metadata_For_Network_Security_v1_1r8.pdf, January 2014.