I.J. Information Technology and Computer Science, **2010, 2, 9-16**
Published Online December 2010 in MECS (http://www.mecs-press.org/)

A Clientless Endpoint Authentication Scheme Based on TNC

Kun Wu
Department of Computer, Beijing University of Posts and Telecommunications, Beijing, China
sherrywukun@163.com

Zhongying Bai
Department of Computer, Beijing University of Posts and Telecommunications, Beijing, China
sherrywukun@msn.com

***Abstract*—Trusted Network Connect (TNC) proposes a hierarchical and scalable architecture to securely and efficiently control endpoints` admission to the trusted computing platform to implement message passing and resource sharing. But, not all endpoints support or run a functional TNC client performing integrity checking, which represents a security risk in lots of environments. We have to consider the problem how to make these "clientless endpoints" access to trusted networks. It is of significance for improving the TNC mechanism. To solve the problem above, under the framework of TNC, this paper comes up with a clientless endpoint authentication scheme named CEAS. CEAS designs five enforcement mechanisms and the related message format to authenticate and authorize clientless endpoints. Furthermore, after the endpoints have connected to the networks, their initial determinations may be dynamically modified according to the updated circumstances. The experiment results prove that CEAS has the capability of effectively and flexibly making clientless endpoints access to trusted networks in a controlled and secure manner.**

***Index Terms*—trusted network connect, network access control, clientless endpoint authentication**

I. Introduction

With the rapid development of trusted computing, we have to consider the problem how to make the whole network to be a trusted computing environment. The traditional security safeguards focus in server and network protection, but ignore security of terminal devices themselves. Most of attacks arise from unsafe terminal devices. So, only building up security architecture from the source of terminal devices, and combining with internal and external factors can construct a trusted and safe network environment [1]. This architecture rejects the network connection of an insecure endpoint, which avoids attackers executing destructive activities.

The TNC Work Group defines an open solution architecture that enables network operators to enforce policies regarding endpoint integrity when granting access to a network infrastructure [2]. The TNC architecture clearly describes how to assess endpoint integrity and enforce compliance when a TNC Client (TNCC) is present on the endpoint.

However, today's networks contain many “clientless endpoints”, legacy devices which do not have a functional TNC client and therefore do not support integrity checking. So, clientless endpoints represent a security risk in a lot of environments because of the lack of identity and integrity information provided by the client.

Aiming at this problem, this paper analyzes current technology used for network admission control. According to the different identity credentials extracted from clientless endpoints, this paper gives five methods to make the TNC entities perform policy assessment for deciding a clientless endpoint whether or not to access a network. What`s more, after the endpoint has connected to the protected network, this paper thinks over how to alter that determination based on updates to the endpoint metadata.

The key point is how to synthesize these enforcement mechanisms to be a clientless endpoint authentication scheme (CEAS), which includes designing and implementing the work flow of CEAS.

The experiment results show CEAS can effectively and flexibly make clientless endpoints access to networks in a controlled and secure manner.

The remainder of this paper is structured as follows: Section 2 introduces the relevant research. Section 3 points out the design of enforcement mechanisms and message format of CEAS. Section 4 describes the deployment and work flow of CEAS. The experiment results are given in section 5. Conclusions and References are given in section 6 and 7.

II. Relevant Research

With respect to TNC, there are many relevant researches having effectively promoted the technology. This paper is inspired.

Reference [3] introduces a method to calculate the “healthy status” of a terminal based on analyzing the real-time characteristics of its behavior and process activity. Based on static characteristics, the strategy could get a better performance, especially, on identifying and isolating the terminals with potential risk.

Reference [4] comes up with a network access authentication model which dynamically computes the trustworthiness of a terminal. When this trustworthiness is below a certain value or the access is overtime, re-authentication mechanism is started.

Reference [5] combines the merits of digital certificate, and uses the probability of authentication session failure to direct the parameters setting in the access control device. This method can effectively promote the control-ability and manageability of network.

Reference [6] presents a network trusted connection attestation model based on the trusted computing platform. The attesting method can verify whether a device is safe and trusted. It is proved to be effective through the CC criterion valuation. Then the attested devices will send requirement to service resource using OSAP protocol, considering the protocol has substitution attack flaw, so a strengthening security method is emphatically proposed.

However, these references just discuss the endpoints` admission from the perspective of integrity checking or authentication protocol with a TNCC. They have not put forward how a "clientless endpoint" could access a trusted network.

Reference [2] gives the TNC architecture for interoperability. As is illustrated in Fig. 1 below, to take a horizontal view on the TNC architecture, there incorporates three layers: the network access layer, the integrity evaluation layer and the integrity measurement layer.

The network access layer has the components whose main function pertains to traditional network connectivity and security. The components found in this layer are the Network Access Requestor (NAR), the Network Access Enforcer (NAE) and the Network Access Authority (NAA).

The function of the components in the integrity evaluation layer is to evaluate the overall integrity of the Access Requestor (AR) with respect to certain access policies, with input from the components at the integrity measurement layer. The components found in this layer are the TNCC and the TNC Server (TNCS).

The integrity measurement layer contains plug-in components whose function is to collect and verify integrity-related information for a variety of security applications on the AR. The components found in this layer are the Integrity Measurement Collectors (IMC(s)) and the Integrity Measurement Verifiers (IMV(s)).

To take a vertical view, there incorporates five roles: the AR, the Policy Enforcement Point (PEP), the Policy Decision Point (PDP), the Metadata Access Point (MAP), and the MAP Client (MAPC).

The AR consists of the three components: the NAR, the TNCC and the IMC.

The NAR is the component responsible for establishing network access. There may be several NARs on a single AR to handle connections to different networks.

The TNCC aggregates integrity measurements from IMC and orchestrates the reporting of local platform and IMC measurements (Integrity Check Handshake).

The IMC measures security aspects of the AR's integrity (e.g. the Anti-Virus parameters on the AR, Personal Firewall status, software versions, and other security aspects of the AR). There is designed for multiple IMCs to interact with a single (or multiple) TNCC/TNCS, thereby allowing to deploy complex integrity policies involving a range of devices.

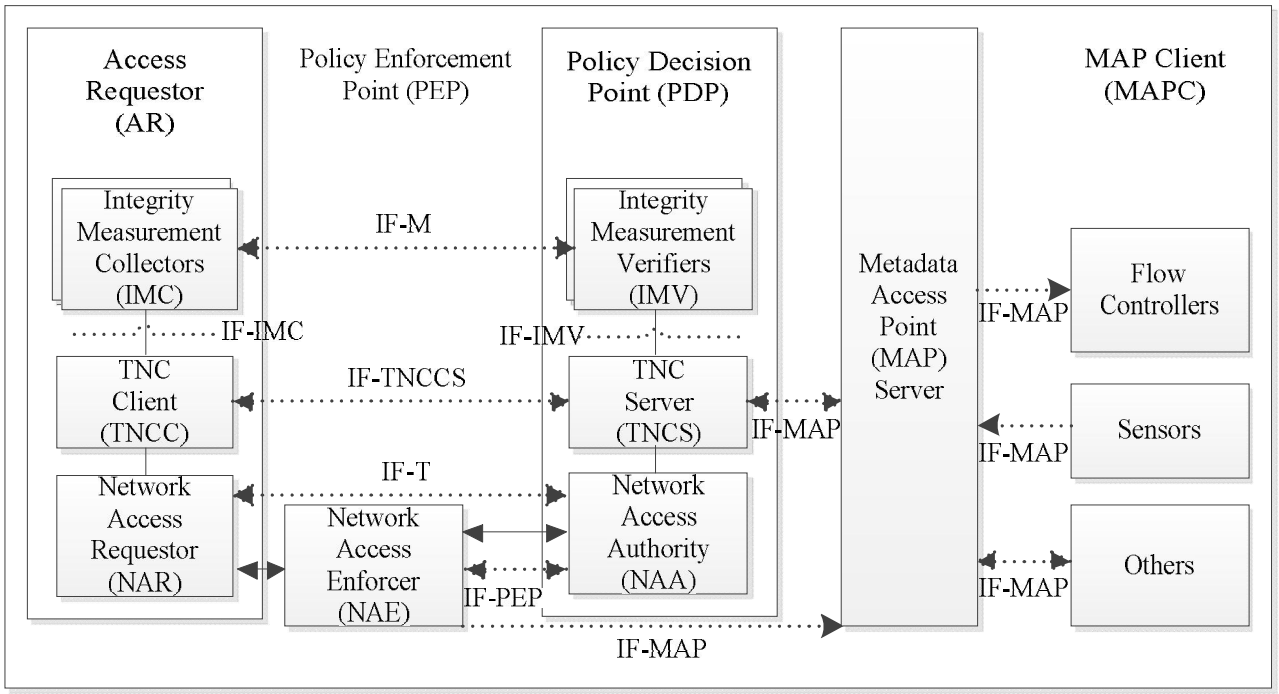

Figure 1. TNC Architecture.

The PEP consists of the NAE component.

The NAE controls access to a protected network, by consulting an NAA to determine whether this access should be granted.

The PDP is composed of the NAA, the TNCS and the IMV.

The NAA decides whether an AR should be granted access. It consults a TNCS to determine whether the AR's integrity measurements comply with the PDP's security policy.

The TNCS manages the flow of messages between IMV and IMC, gathers IMV Action Recommendations from IMV, and combines those recommendations (based on policy) into an overall TNCS Action-Recommendation to the NAA.

The IMV verifies a particular aspect of the AR's integrity, based on measurements received from IMC and/or other data.

The MAP is composed of the Metadata Access Point Server (MAPS).

The MAPS is a component to which other TNC components may publish, subscribe, and search data. These data reflect the state of TNC elements and aid in decision making and policy enforcement.

The MAP Clients comprise the Flow Controller and the Sensor.

The Flow Controller makes and enforces decisions about network activities utilizing information from the MAP.

The Sensor monitors network activities and publishes information to the MAP.

The interfaces which will be standardized are depicted by named lines, such as IF-T, IF-PEP and IF-MAP. They define relationships, protocols and exchanged messages between components.

On the whole, the AR requests access to a protected network. The PDP compares the AR's credentials and security posture information against certain policies. Then, it decides how to authorize the AR. If the PEP is present, the PDP then communicates its decision to the PEP which actually grants or denies access. Optionally, the MAPS is used to aggregate information about devices, for instance, network traffic, management, and security data. The MAPCs, which might not be directly involved with the decision, may coordinate with both the PDP and the PEP in monitoring and enforcing network security policy compliance.

Because endpoints in the absence of a TNCC do not support integrity checking, this paper utilizes a subset of the standard TNC components to provide a range of security measures for clientless endpoints. That is, TNCC, TNCS, IMCs and IMVs are unavailable. And, the PDP and PEP may be separate, individual devices in a network or may be combined in a single network device.

We have researched current technology used for network admission control. After analyzing the identity credentials extracted from clientless endpoints, we propose five enforcement mechanisms to authenticate and authorize the endpoints. By means of the specific message passing, a new authentication scheme (CEAS) is brought forward.

III. Key Technology of CEAS

A. Enforcement mechanisms of CEAS

By analyzing the existing protocols for network access, in the light of the extracted information of endpoints, here, the Enforcement Mechanisms (EM(s)) controlling clientless endpoints` connection are divided into five classes as follow:

EM 1: Local Authorization.

Judging by a MAC or IP address specific rule resident on the PEP for individual devices and provision access, the PEP is capable of checking whether an endpoint has a registered or unregistered MAC/IP address. It refers valid credentials but unverifiable integrity for an authenticated endpoint as well.

The related devices may be an endpoint logging into a Windows domain in an environment where an inline PEP is able to intercept the Windows login, an endpoint running an 802.1X supplicant but no TNCC, or a laptop running a TNC stack which is configured not to share information with the network.

EM 2: RADIUS-Based 802.1X [8] Authentication.

The 802.1X standard is a layer 2 protocol executing access control and identity authentication based on Client/Server. It makes a distinction between controlled logic ports and uncontrolled logic ports. The service messages exchange directly and normally via controlled ports. Only EAP messages with identity credentials can be transmitted via uncontrolled access ports. At this time, RADIUS and switch together can impose restriction and authorization on users/devices connecting to LAN/WLAN. Different users/devices can be mapped into different VLANs (Virtual Local Area Network(s)).

In this EM, it refers invalid credentials which can`t authenticate an endpoint. For example, an unknown or failed MAC address, IP address or Identity.

There are two cases of invalid authentication: one is an 802.1X-capable endpoint configured for another environment that does not share a trust relationship with this being accessed; another is an 802.1X-capable endpoint connecting to a non-802.1X-enabled network device.

EM 3: RADIUS-Based MAC Authentication.

This is primarily used in 802.1X environments to handle non-802.1X-enabled endpoints. It refers to some completely unresponsive data, including unserviceable MAC address, IP address, or behavior.

The related devices may be a badge reader, a printer, a networked security camera, or a laptop with a wireless client. This situation involves an IP-enabled security camera with no LLDP-MED support.

The authentication is determined by whether a MAC address is registered or not, and without verification against an external database or MAP. By this means, an unknown or unregistered MAC will trigger limit access to an isolation area (VLAN) to register a new MAC address.

The identity credential is mainly the pair of username/password. Three formats are used:

MAC Address/[empty]

MAC Address/MAC Address

MAC Address/[secret]

EM 4: Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) [9] Authorization.

LLDP (IEEE802.1ab) is a link-layer protocol that allows a network device to transmit advertisements containing device information, device capabilities and media specific configuration information. In this way, a network device can inform other nodes on the network that it exists. The LLDP agent operates only in an advertising mode. Hence, it does not support any means for soliciting information or keeping state between two LLDP entities.

The advertisements can come into being different TLVs (Type/Length/Value(s)) which are encapsulated in the LLDP Data Units (LLDPDU(s)). The LLDP agent periodically advertises information over LLDPDUs to neighbors attached to the same network. The neighbors record the information received from other agents in IEEE-defined MIB (Management Information Base) modules, which can be used to query or estimate the communication situation of links.

LLDP-MED is an enhancement to LLDP to support the automatic configuration of resources for media-enabled devices providing "plug and play" networking. It is very suitable for the location of adding, moving and updating frequently. The new TLVs will offer PoE (Power over Ethernet), network policy, and the media endpoint location and inventory of Emergency Call Service (ECS). Especially, network policy permits the endpoint and switch to publish their VLAN IDs.

The related devices may be a PC running a VoIP softphone, an IP phone, a conference bridge, a media gateway, or a media server.

A layer 2 network device acting as a combined PEP/PDP may make use of LLDP-MED for specific attributes to determine and apply permissible levels of access control. The PEP/PDP may maintain a table of LLDP-MED device types to authorize a pre-determined VLAN for specific endpoints (e.g. mapping VoIP devices to a phone VLAN and IP video camera devices to a camera VLAN).

This layer 2 PEP/PDP can report LLDP-MED TLVs via SNMP or syslog to a MAP. These TLVs are shown in Table I below. The remaining TLVs which should be reported are shown in Table II.

EM 5: DHCP Authorization.

Dynamic Host Configuration Protocol (DHCP) is a LAN protocol based on UDP. It is used to automatically allocate IP address for devices connecting to internal networks.

By applying DHCP snooping and/or dynamic ARP inspection, the PEP can generally utilize a static local data store (MAC/IP address for per-port or per-SSID) to identify unresponsive and/or unrecognized endpoints after timeout. On the one hand, the Option82 field contains MAC address, Port ID, and VLAN ID. On the other hand, the Option60 field contains Vendor, and Service Option that represents the endpoint type.

TABLE I.
TLVS REPORTED BY PEP/PDP

TLV	Type	OUI	Subtype
Chassis ID	1		
Port ID	2		
Time To Live	3		
End of LLDPDU	0		
LLDP-MED Capabilities		00-12-BB	1
Network Policy		00-12-BB	2
Location Identification		00-12-BB	3
Extended Power-via-MDI		00-12-BB	4

TABLE II.
THE REMAINING TLVS WHICH SHOULD BE REPORTED BY PEP/PDP

TLV	OUI	Subtype
Inventory-Hardware Revision	00-12-BB	5
Inventory-Firmware Revision	00-12-BB	6
Inventory-Software Revision	00-12-BB	7
Inventory-Serial Number	00-12-BB	8
Inventory-Manufacturer Name	00-12-BB	9
Inventory-Model Name	00-12-BB	10
Inventory-Asset ID	00-12-BB	11

It is commonly used to allow endpoints which may not have a functioning 802.1X supplicant or LLDP agent access to a network. When all other EMs are unavailable or have failed, the method will come into force.

The priority of the EMs may be configurable and adjusted. There is a default priority among them in accordance with their importance. The PEP or PDP should be capable of implementing the default priority ("1" is the highest) shown in Table III.

Fig. 2 illustrates how a CEAS PEP implements these EMs when a clientless endpoint connects.

On the other hand, after a clientless endpoint has been authenticated successfully, it is authorized to use resources or services in the trusted network. The levels granted are designed as follows [7]:

Override

Static MAC/IP bypass

Internet only

Remediation server

Default guest VLAN

Filter

Restrictive ACL (Access Control List)

B. Message format of CEAS

The CEAS message transmits information between PEP and PDP. Its format is shown as Table IV.

TABLE III.
DEFAULT PRIORITY OF EMS

Priority	EM	Authentication	Extracted Data
1	Local Auth	Device identity	MAC/IP address, Port ID
2	802.1X Auth	User identity Device identity	Identity credential (EAP message)
3	MAC Auth	Device identity	MAC address
4	LLDP-MED Auth	Device identity, Device class	TLVs (SNMP/syslog)
5	DHCP Auth	Location only	MAC/IP address, Port ID

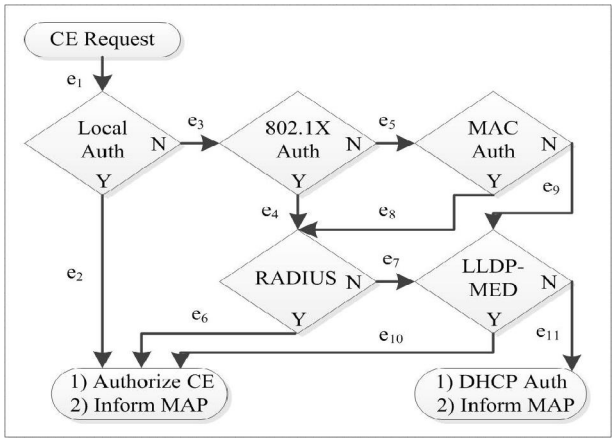

Figure 2. Work flow of EMs with default priority.

TABLE IV.
CEAS MESSAGE FORMAT

Code	Identifier	Length	Type	TypeData

The Code field occupies 1 byte. It indicates the type of packet. When the value of Code is 1, it is a Request packet. On the contrary, when the value is 2, it is a Response packet.

The Identifier field occupies 1 byte. It indicates every Request matches a sole Response. When a Request is replayed after timeout, its value must be the same. Any new (non-replay) Request must modify the value. If a replayed Request is received and the matched Response has been sent, the Response must be replayed. At the moment of responding the first Request, the replayed Request will be discarded.

The Length field occupies 2 byte. It indicates the length of packet.

The Type field is 1 byte. It indicates the EM applied currently. The value must be same in the matched Request and Response. But, when current EM is invalid, Response will be filled in the value of next EM type on the default priority shown in Table III.

The TypeData field of Request is 0 or more byte. Its format is decided by the Type.

The TypeData field of Response include as follows:

MAC address of endpoint

Time of authorization

Identity of device provisioning access (IP address of combined PEP/PDP)

Location of endpoint (interface or SSID to which endpoint is connected)

Authorization level granted

During the whole course of communication, all the messages are enciphered and encapsulated, which ensures the related information are confidential and integral. Further, the timestamp is used to resist the replay attack. Trusted Computing Group (TCG) has issued the specification of TNC IF-T: Binding to TLS [10].

IV. CLIENTLESS ENDPOINT AUTHENTICATION SCHEME

As illustrated in Fig. 3 below, the basic components of CEAS are: the clientless endpoint itself, an enforcement point applying policy to the endpoint (a PEP), a policy server determining what policy is applied (a PDP), and, in some environments, a metadata clearinghouse (MAP) providing information that can inform a policy decision and other network devices contributing metadata (Sensors).

A PDP makes policy decisions and provisions them to a PEP over IF-PEP. A PEP consumes policy decisions from a PDP via IF-PEP and enforces those decisions. The access control device may be a standalone PEP, or a combined PEP/PDP.

A combined PEP/PDP is a single network device performing both PEP and PDP functions, which makes an independent access control decision, using static local configuration.

A standalone PEP might be a switch or VPN concentrator without any local access control configuration, which must consult a PDP or a MAP respectively to obtain policy. The PDP may also act as the AAA data store, consulting an internal database of credentials or MAC addresses, or it may consult an external AAA data store such as an Active Directory server, LDAP database of MAC addresses, separate guest access management or endpoint profiling solution.

A MAP is a metadata access point. Metadata could be information about flows in a network, or information about a specific endpoint that has connected to a network.

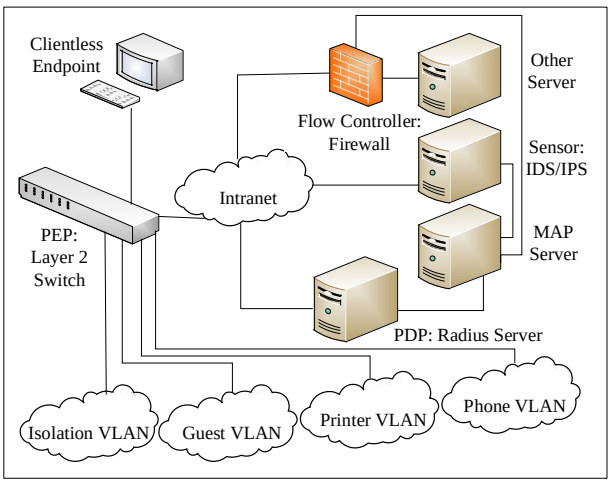

Figure 3. CEAS network deployment.

This metadata can be used to express device classification. A Sensor other network device contributes metadata publishes information to a MAP via IF-MAP.

In addition to validate the authentication credential or endpoint identifier, a PDP may also consult a MAP to determine whether any additional metadata (such as behaviors, results of a vulnerability scan to IDSes, DHCP allocation, traffic logs, etc.) is available to inform the access control decision.

For an initial connection to a network, this metadata may not yet have been collected. Once the initial access control decision has been made and enforced, the PDP may subscribe to the MAP for information about that endpoint.

After the endpoint has connected to the network, circumstances may change. Firstly, the initial admission policy may have modified. Secondly, the endpoint`s identity may have changed. Thirdly, the Sensors may have detected inappropriate or unauthorized activity. Under all these conditions, there requires a re-evaluation of the endpoint's access privileges. The Sensors will publish the related information to the MAP, and then the MAP notifies the PDP. In line with the MAP data or static access control configuration, the PDP probably restricts or terminates the endpoint's initial access permission. The PDP publishes the new authorization information to the MAP in order to inform the Sensors to modify the access policy.

TCG has issued two specifications concerning the MAP. One is the specification of TNC IF-MAP Metadata for Network Security [11]. The other is the specification of TNC IF-MAP Binding for SOAP [12].

The work flow of CEAS is shown as Fig. 4. The steps marked the asterisk (*) are other ones at the same execution level.

Flow 1: The Clientless Endpoint (CE) initiates a connection request.

Flow 2: Upon receiving a network connection request, the PEP extracts the related information about the CE, forms the network access decision Request message and sends the message to the PDP.

Flow 3: The PDP authenticates the user/device identity credential, forms the authorization level granted Response message and sends the message to the PEP. Besides, the PDP publishes information about the CE to the MAP via IF-MAP.

Flow 4: The PEP receives the Response message from the PDP, and check the Type field whether is the same as the matched Request message. If they are same, it enforces the network access decision by the PDP. Otherwise, it will enforce the required EM type in the Response message, collect the related information and send a new Request to the PDP.

In order to prove the validity and security of CEAS, this paper designed and implemented the prototype in simulation. Moreover, the relevant experiments have been finished.

V. Results and Analysis of Experiments

In the light of Fig. 3, the environment of experiments has been set up.

The layer 2 switch has configured a local rule to allow the MAC address (11-22-33-44-55-66) to Intranet and the Port 1 to a Printer VLAN. It maintained a table of LLDP-MED device types to map VoIP devices to a Phone VLAN and the device (System Name=PC2 and Inventory-Serial Number=1) to a Guest VLAN. Also, it deployed a default access policy to allow unknown devices to an Isolation VLAN.

The RADIUS server has registered the usernames and passwords (PC1/1, 22-33-44-55-66-77/[]).

There are three experiments about CEAS.

Experiment 1: There are nine test cases which cover all the paths in Fig. 2 to simulate clientless endpoints to access network as shown in Table V. Table V turns out that CEAS is effective.

Experiment 2: There are seven devices having been permitted to access the restricted network. Yet, circumstances change. As is shown in Table VI below, some devices` identities are modified privately, for example, the CEs` name or MAC address; Some device makes its own connection to another port not being allocated to it; Some updated initial admission policies make the inline devices terminated; Again, the Sensors monitor that some abnormal activities which maybe threats for network security are happening. Consequently, the PDP makes decision to terminate the devices.

Because of the breadth and volume of information that a MAP can make available to the decision-making

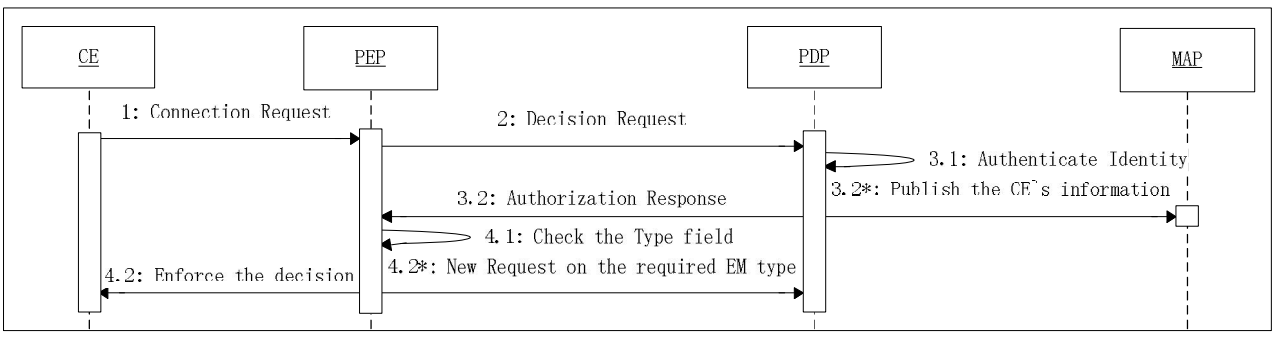

Figure 4. Work flow of CEAS.

TABLE V.
CEAS TEST CASES

CE	Data	EM	Authorization	Path
Desktop1	11-22-33-44-55-66	Local Auth	Intranet	e_1e_2
Desktop2	CE1/Port1	802.1x Auth	Intranet	$e_1e_3e_4e_6$
Laptop1	CE2/Port2	LLDP-MED Auth	Guest VLAN	$e_1e_3e_4e_7e_{10}$
Laptop2	CE3/Port3	DHCP Auth	Isolation VLAN	$e_1e_3e_4e_7e_{11}$
Printer1	22-33-44-55-66-77	MAC Auth	Printer VLAN	$e_1e_3e_5e_8e_6$
VoIP Phone1	33-44-55-66-77-88	LLDP-MED Auth	Phone VLAN	$e_1e_3e_5e_8e_7e_{10}$
Printer2	Port4	DHCP Auth	Printer VLAN	$e_1e_3e_5e_8e_7e_{11}$
VoIP Phone2	44-55-66-77-88-99,LLDP-MED Capabilities =VoIP	LLDP-MED Auth	Phone VLAN	$e_1e_3e_5e_9e_{10}$
Camera	None	DHCP Auth	Isolation VLAN	$e_1e_3e_5e_9e_{11}$

TABLE VI.
MAP TESTS OF CEAS

CE	Initial Data	Changed Data	Decision
Device1	11-22-33-44-55-66	22-33-44-55-66-77	Terminate
Device2	CE2/Port2	CE1	Terminate
Device3	CE3/Port3	Port1	Terminate
Device4	CE4/Port4	CE2/Port3	Terminate
Device5	Permitted to connect to Port5	Not permitted to connect to Port5	Terminate
Device6	Normal status	Abnormal status (malicious attacks)	Terminate
Device7	22-33-44-55-66-77	None	Keep

process, the MAP-enabled environment provides the greatest confidence in the security of access control for clientless endpoints.

Experiment 3: In view of common network attacks, such as message tamper, Man in the Middle (MitM) attack, test finding and blocking ability of the system. There performed 10 groups of tests, and 10 times of attacks in every group. Fig. 5 illustrates the statistical results. The success ratio in every group is above 70%. In this way, CEAS is able to effectively prevent from the network attacks, which ensures the security of the system.

From what has been discussed above, on the basis of the obtained data, CEAS can enforce the relevant mechanisms to implement network access control with regard to clientless endpoints.

VI. CONCLUSIONS

Nowadays, it is a real security requirement extending the trusted computing mechanism into networks to build a trusted computing environment. The TNC Work Group defines an open solution architecture to enforce policies

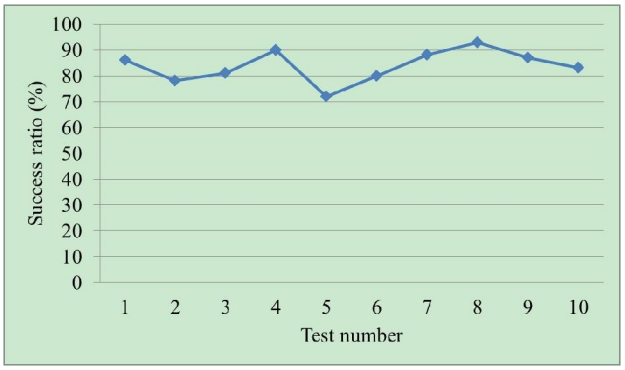

Figure 5. Statistical result of anti-attack ability of the system.

regarding endpoint integrity when granting access to a network.

Nonetheless, there are a number of endpoints which do not support or run a TNCC and therefore do not check integrity, which means a security threat for protected networks. Thus, it is necessary and significant to research a secure and efficient method to make clientless endpoints permitted to access trusted networks. This will help to expand the trusted resource sharing.

Taking into account characteristics of existing authentication technology, this paper proposes a new authentication scheme (CEAS) to gain a clientless endpoint`s identity information upon different protocols. CEAS utilizes five enforcement mechanisms to authenticate and authorize the endpoint to access a network via a custom message. Meanwhile, for a MAP is added to the environment, the scope of the access control scheme is considerably increased. Thus, network security policies can be enforced based on multiple dynamic pieces of information. Besides, message encryption and timestamp prevent the network from attacks.

The experiments simulate the environment and conditions of clientless endpoint access control. Two experiments are designed to verify the validity of enforcement mechanisms and MAP dynamic decisions. The last experiment takes the ability of the system resisting common network attacks into account. The results prove CEAS can control effectively and flexibly clientless endpoints to connect with network in most cases, and avoid the inline computers being attacked.

In addition, CEAS is easy for vendors to adopt and extend, which enhances interoperability and enforce compliance in TNC environments.

For improving the TNC mechanism further, the future work of CEAS may go on with security constrained policies and the methods of monitoring and auditing the system. They will make network access control more secure and effective.

ACKNOWLEDGMENT

Jiancheng Qin at Beijing University of Posts and Telecommunications gave this paper much prudent and helpful suggestion of improvement. Hereby, thank him very much.

REFERENCES

[1] ZHANG HuanGuo, CHEN Lu, and ZHANG Liqiang, "Research on Trusted Network Connection," *Chinese Journal of Computers*, vol. 33, pp. 706 717, April 2010, (In Chinese).

[2] TCG Trusted Network Connect, "TNC Architecture for Interoperability Specification Version 1.4 Revision 4," http://www.trustedcomputinggroup.org/files/resource_files/51F9691E-1D09-3519-AD1C1E27D285F03B/TNC_Architecture_v1_4_r4.pdf, May 2009.

[3] LIU Weiwei, HAN Zhen, and SHEN Changxiang, "Trusted network connect control based on terminal behavior," *Journal on Communications*, vol. 30, pp. 127–134, November 2009, (In Chinese).

[4] YIN Jianchun, SI Zhigang, and CHANG Chaowen, "Research on trustworthiness computing-based network access authentication model," *Computer Engineering and Design*, vol. 29, pp. 4417–4419, September 2008, (In Chinese).

[5] LIU Wei, YANG Lin, DAI Hao, and HOU Bin, "A New Network Access Control Method and Performance Analysis of Authentication Session," *Chinese Journal of Computers*, vol. 30, pp. 1806 1812, October 2007, (In Chinese).

[6] XIAO Zheng, LI Jingxia, LIU Xiaojie, CHEN Jun, and HOU Zifeng, "Design and Research of a Trusted Network Attestation Model and Improved OSAP Protocol," *Computer Science*, vol. 33, pp. 56 60, 2006, (In Chinese).

[7] Richard Froom, Balaji Sivasubramanian, Erum Frahim, *Building Cisco Multilayer Switched Networks (BCMSN) (Authorized Self-Study Guide)*, 4rd ed., USA: Cisco Press, 2007.

[8] IEEE Computer Society, "Port-Based Network Access Control," *IEEE Std 802.1XTM-2004*, December 2004.

[9] Telecommunications Industry Association, "Link Layer Discovery Protocol for Media Endpoint Devices," *ANSI/TIA-1057-2006*, April 2006.

[10] TCG Trusted Network Connect, "TNC IF-T: Binding to TLS Specification Version 1.0 Revision 16," http://www.trustedcomputinggroup.org/files/resource_files/51F0757E-1D09-3519-AD63B6FD099658A6/TNC_IFT_TLS_v1_0_r16.pdf, May 2009.

[11] TCG Trusted Network Connect, "TNC IF-MAP Metadata for Network Security Specification Version 1.0 Revision 25," http://www.trustedcomputinggroup.org/files/static_page_files/FCED7251-1A4B-B294-D000EDCD8C39D226/TNC_IFMAP_Metadata_For_Network_Security_v1_0r25.pdf, September 2010.

[12] TCG Trusted Network Connect, "TNC IF-MAP Binding for SOAP Specification Version 2.0 Revision 36," http://www.trustedcomputinggroup.org/files/static_page_files/1528BAC2-1A4B-B294-D02E5F053A3CF6C9/TNC_IFMAP_v2_0r36.pdf, July 2010.

Kun Wu, born in 1980. Since 2009, she has been a Ph.D. candidate in computer science and technology from Department of Computer, Beijing University of Posts and Telecommunications, Beijing, China. Her current research interests include information security, trusted computing and access control. She achieved the master degree in Software Engineering from Jilin University, Changchun, China in 2005. Moreover, she has published three academic papers.

Zhongying Bai, born in 1941. He is professor and doctoral supervisor of Department of Computer, Beijing University of Posts and Telecommunications, Beijing, China. His main research interests are computer architecture, and network security collaborating with Professor Yixian Yang. And, he has published 22 books and more than 50 academic papers.

