www.sensorsportal.com

Sensors & Transducers

© 2014 by IFSA Publishing, S. L.
http://www.sensorsportal.com

Analysis and Comparison on Novel Sensor Network Security Access Technology

Ping LIU
Computer and Information Engineering Institute, Nanyang Institute of Technology,
Henan Nanyang, 473004, China
Tel.: 13525661045
E-mail: eduliuping@163.com

Received: 4 November 2013 /Accepted: 9 January 2014 /Published: 31 January 2014

Abstract: The article introduces against technical defects of traditional network access control system, detail NAC, NAP, UAC and TNC four kinds of new network security access technology, and this article analyzes and compares them. Security framework for wireless sensor networks SPINS defines the mechanism and algorithm of complete and effective in confidentiality, point-to-point message authentication, integrity, authentication, broadcast authentication. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Network security access, Analyze, Compare.

1. Introduction

With the rapid development of computer networks, security threats of networks and terminal computer were tested explosive growth each day, the mainstream application platform has thousands of security vulnerabilities [1]. Traditional terminal computer security technology is protecting the attack terminal, in the same, the protection of intranet security and usability has become stretched. Faced with an increasingly complex enterprise network security status, the application of management to control the enterprise information system network, and improving the level of IT internal control, is an important issue which enterprises are currently facing and need to solve.

Inevitably, frequent exchanges between enterprises and outside will inevitably lead to more and more outside users into intranet, business executives are increasingly difficult to control the user to log into the corporate network terminal equipment, in fact, at present business prevalence has difficulty to monitor external computer access to internal network, and external users freely access the intranet network, most likely make some malicious user intrusion the internal network in the case of companies ill-informed, resulting in sensitive data leaks, the virus spread and other serious consequences, legitimate users' terminals within the enterprise, the same will give enterprise internal network security risk, if there is not in time to upgrade the system patches and virus and install software from unknown sources could lead to a internal network security risks to the enterprise network security and a heavy blow.

Wireless sensor network node does not have a unified logo, nodes to exchange data through radio, multi hop communication; a large number of nodes, the random distribution, with large, the network topology changes dynamically over time, node energy of each power supply Co., short life cycle. So WSN need to study new technologies, in order to ensure the realization of the network energy consumption minimization, node lifetime maximization, energy load equalization, and communication optimization.

Flooding attack is a new type of attacks in sensor network method. Many protocols require nodes to broadcast HELLO packets to its adjacent nodes broadcast their. The attackers used transmission power broadcast routing is large enough or other information, which makes every node in the network that the attacker is its neighbors. In order to use the HELLO flooding attack the attacker does not need to construct legal communication. An attacker can simply use a large enough power to replay hacking (Overheard) into the package, so that every node in the network can receive.

Network access control technology is in such demand emerged, network access control technology can ensure that all devices to access network resources to be effective security control, resist all kinds of security threats to effect network resources, improve corporate governance and production efficiency [2]. It makes all the network access layer devices enhance a safe point, and terminal equipment must meet certain security and policy conditions before they can access through the routers and switches to access the network. This can greatly eliminate the worms and virus on the Internet more and more serious threat to the business and influence, to help customers discover, prevent and eliminate security threats.

2. Traditional Sensor Network Access Control Technology

Traditional network access control technology mostly based on the "Scan-found-block" work mode, through the management center of network access control system, constantly scan the network, and validity check the scanning computer, Judge the terminal whether is a legitimate or not. When they find that the terminal is not legal, linkage with the switch or the uses of ARP spoofing, etc., block the terminal access network.

For the existence of sensor networks in the sewage tank attack, the use of link layer encryption and authentication can prevent most routing protocols of external attack, the attacker difficult to join the network topology; sewage tank attack is very difficult to reach. At present, in the routing layer based on the routing protocols are designed to effectively prevent the precision. Geographic routing protocol can effectively defense the sewage tank attack.

The network access control system achieved by this principle is technical defects:

1) Illegal terminal can survive for some time in the network.

Due to the need for all addresses in the whole network to scan, for each address have a certain interval scan cycle, so this time illegal access terminals in the network can survive a certain time, and during this time, the attacker may have completed part of the attack [3]. And as the network grows, the time interval for each scan revealed extension of the illegal terminal on the network to survive longer, the greater the threat for the network.

2) System can not find the illegal terminal in some cases.

a) For need to specify the scan network range, when the address which the illegal access terminal used outside the specified scanning, the system can not "find" illegal access devices.

b) When system is testing by using PING, TCP connections, etc. if the illegal access devices installed personal firewall, and enabled the corresponding security rules, the system can not "find" the illegal terminal access.

c) Illegal access terminal can modify its own IP address and MAC address, impersonate legitimate terminal access to the network, the system can not "discovery" this counterfeiting [4].

3) Consume valuable network resources.

Access control system needs to be constantly scanning the network to detect illegal access terminal, which will consume a large amount of valuable network resources, especially in large networks, this problem is more prominent.

To solve the selective forwarding attack directly scheme is used to evaluate the detection mechanism, the behavior of the node to node, make malicious behavior beyond the normal standard, the base station or the cluster head to the malicious nodes out of the network, not to participate in the normal network communication. Indirect scheme is the use of redundant paths, namely multi path routing methods, this approach can deal with multiple attacks.

Key distribution, ordinary nodes, update the negotiation is done through the cluster head. The characteristics of distributed key management is the key to realize through the cooperation of neighboring nodes distribution, has better property. The characteristics of hierarchical key management is low computational requirements of ordinary nodes, storage capacity, but damaged the cluster head will lead to serious security threat.

3. Current Mainstream Network Access Control Technology

Against technical defects of traditional network access control technology, Present the new type of network access control technology turn the control target to computer terminals, start from the terminal, through the security policy specified by the administrator, for access to private network hosts for safety testing, automated refuse unsafe host access, protect network until the hosts meet the security policy of the network. Current representative techniques include: network access control technology (NAC), network access protection technology (NAP), trusted network connection (TNC) and universal access control (UAC).

3.1. NAC Technology

NAC is a set of protocols which can be used to define how to protect security of network and nodes before nodes access the network [5]. NAC also integrated automated treatment process, allowing network equipment (such as routers, switches, firewalls, etc.) in close collaboration to support the server and end-user's computer, to protect the information system to be safely operating before interactive.

NAC has become an important tool to stop potential spy and attackers, can also be used to manage more complex web licenses and authorizations, permits and authorizations can be adapted to these different groups of users to access different parts of the network. This technology helps companies seeking to enhance their network access for any individual or device security policy. NAC also helps regulations of businesses with external and internal policies to maintain consistency, to protect network resources from evolving network threats.

1) Target of NAC.

NAC represents a security product; the objective can be divided into the following three parts:

a) Reduce the risk of zero-day attacks. The key values of NAC solution is to prevent the terminal lack of anti-virus, patch, host intrusion prevention software access to network resources, and may prevent the device from other computers at risk.

b) Enhance the strategy [6]. NAC solution allows network operators to define policies, such as user role allowed access to the network or the type of computer, and strengthen these strategies in switches, routers and other network devices.

c) Identity and access management. The traditional IP network enhance access policies according to IP address, NAC environment enhance the security according to user.

2) Composition of NAC.

NAC consists of the following:

a) Trust Agent.

It exists in the terminal system, responsible for collecting security state information of security software for different customers. This section integrated anti-virus software products [7]. TA is integrated in the Cisco Security Agent and uses it to assess the operating system version, patch level, and Hot Fix information, and transmit such messages to the CTA. There the host which is no proper upgrade will be limited to or refuse access to the entire network.

b) Network Access Equipment.

It can forced control those equipment requesting access to implement security measures, including routers, switches, wireless access terminals and security equipment. These access devices require host security requirements "Credentials", and according to that information to develop specific server access policies. According to Policies customer required, the network will implement appropriate allow access control measures.

c) Policy server.

It is used to assess the safety performance information from the terminal, to determine the access request from them take appropriate measures. Specific product is the Cisco Secure Access Control Server (ACS), which is an authentication, authorization and recording of the RADIUS server, compose the policy server system. It is based on Cisco NAC to work, to run concurrently with the application server, to provide a deeper level of confidence in recognition, such as anti-virus policy server.

d) Management system.

A specific product is Cisco VPN / Security Management Solution (VMS). Meanwhile, Cisco Systems safety information management solutions provide display and reporting tools [8]. NAC also provides collaboration management solutions for terminal security software.

Cisco NAC can operate all of the network access host, including campus switching, wireless and wired routing, WAN and LAN connections, IPSec connection, remote connection and dial-up access. Before allowed remote access to corporate resources, NAC help sure that remote access and mobile devices whether have the latest anti-virus updates and operating system patches upgrade.

3) Treatment strategy of NAC.

NAC has two treatment strategies, one is the network isolation, and the second is to limit the network entrance.

An isolated network is a restricted IP network; it can provide users with some selective access of the host and application. Isolation is usually assigned to the VLAN implementation. When NAC product considers that one end user is "time out", the switch port will be assigned to a VLAN, this VLAN connected to patch and update servers, but can not connect to the rest of the network. In addition to VLAN solution, also can use address management techniques to achieve isolation, to avoid the high cost of VLAN management.

Limit the network entrance can intercept the HTTP request reached webpage; Guide user to a web application which can provide instructions and tools of computer update. Until the computer through the automated check, in addition, the network applications outside the network entrance are not licensed.

4) Type of NAC.

Many vendors can provide NAC technology and products, there are many types. According to their primary method used, NAC can be divided into the following types:

a) Agent-based NAC: NAC products rely on software installed on the endpoint device, the so-called agent. This agent communicates with a NAC server or device connecting with network. This method is relatively simple, but less flexible, and requires install and run specific software on the terminal equipment.

b) Agent less NAC: This method does not require install a particular agent on the personal desktop and notebook computers and other terminal devices. In contrast, the agent is stored in a temporary directory. Does not use proxy make deployment easier, and simplify the operation of NAC.

c) Inline NAC: the run of NAC like a firewall in network access layer, it was in charge of all clients communication through it, and can enhance the security policy [9]. This method is relatively simple, but it will produce throughput bottleneck in a larger network. This approach will over time caused by increased costs, because the traffic increase, it will be asked to add more inline devices.

d) Of-band NAC: This method uses existing infrastructure to enhance performance, it typically is distributed, because the client transmit data to a central console, to enhance the strategy.

3.2. NAP Technology

NAP is a security mechanism built into Windows Server2008 and Windows Vista client and its subsequent versions of the operating system. NAP allows users to monitor security status of any computer which attempts to access the user's network, and ensure access computer has security preventive measures meet the user's health policy [10]. The computers which not meet the user's health policies will be access to a restricted network environment; users can store some security software in the network environment, to help these poor security computers improve to security level meet the user requirements.

1) Role of NAP.

a) Monitor whether computer access to the network meets the requirements of health policy, enforce health requirement strategy on the computer;

b) Ensure computer access to networks meets the policy, the computer which does not meet the requirements of security policy, is limited to a restricted network;

c) Provide updated support for the computer which does not meet the health requirements, automatic update computers to meet the requirements of security policy.

2) Work process of NAP.

The process of NAP is to enforce the client to execute; NAP working process is shown in Fig. 1.

a) The client access to the local computer network;

b) The client's status will be passed to the backend Network Policy Server;

c) Network Policy Server will contrast the client state received and the pre-contrast on policy server;

d) The unhealthy computer which does not meet the policy requirements will be access to restricted network which provide a patch server to repair the unhealthy computer state;

e) The computers which meet the policy requirements or repaired will be access to intranet, have unlimited access.

3) Basic structure of NAP.

The NAP in Windows 2008 environment is typical client/server architecture, the basic structure is shown in Fig. 2.

a) Customer environment include SHA (System Security Agent), QA (Quarantine Agent) and EC (Enforcement client). SHA check and declare the health status of customers (patch status, virus signatures, system settings, etc.), each SHA define a system health requirements or a group of system health requirements; force the client to use the enforced method, each NAP EC is defined for different types of network access or connection.

b) Repair server is used to install the required updates, settings and applications, turn the client computer to health state, the computer which does not meet the inspection requirements of the SHA is routed to the repair server [11].

c) Network access equipment is equipment which can give or deny the customer's request for access to the network.

d) System health server provide strategy which the client must be followed by defining the health requirements of the system components on client

e) NPS server includes QS and security checks. QS sits is in the IAS Policy Server, perform the match action after SHV checked, SHV check the declaration generated by security agent.

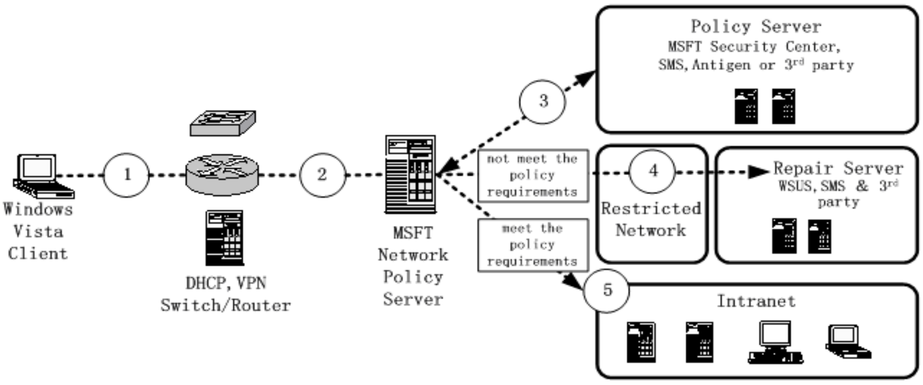

Fig. 1. The work process of NAP.

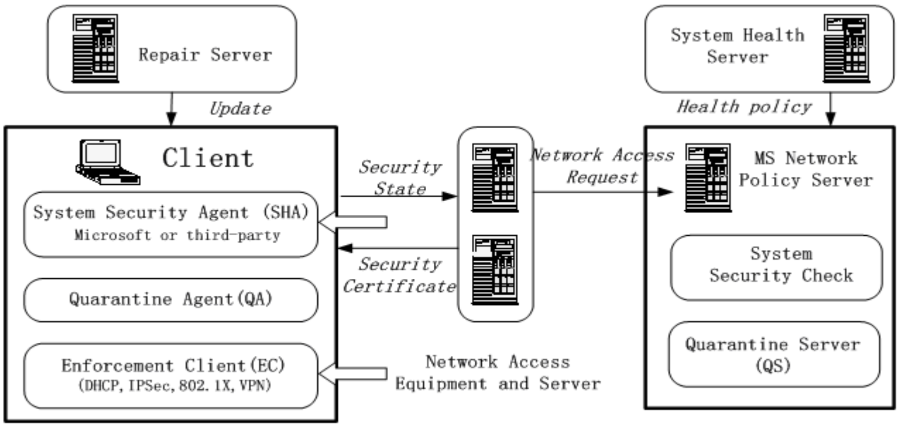

Fig. 2. The basic structure of NAP.

In order to check the health of the host to access the network, network architecture needs to provide the following functional areas:

1) Health policy validation: determine whether the computer adapt to the health strategy.

2) Network Access restrictions: limit computer access strategies suited.

3) Automatic remedy: provide necessary upgrade to the computer which dose not meets the strategies, to adapt to the health strategy.

4) Dynamic adaptation: automatic upgrade adaptive strategy computer so that it can keep up with health strategy update.

3.3. TNC Technology

TNC is an expansion of credible platform applications, also is a trusted computer system and network access control mechanism combination. It refers that before the terminal access network, authenticate the user's identity; If authenticated, authenticate the identity of the terminal platform; if authenticated, measure the credibility state of terminal platform, if the measurement results meet the network access security policy, terminal is allowed to access network, Otherwise terminal is connected to the designated quarantine area, security patched and upgraded [12]. TNC aims to continue the terminal credibility state to network, expand the trust chain from the terminal to the network. TNC is an implementation of network access control method, is a proactive method of defense, can suppress most of potential attack before it occurs.

1) Function of TNC.

TNC's main purpose is to provide a framework composed by a variety of protocol specification to achieve a diverse network standard, which provides the following functions:

a) Platform Certification: used to verify the identity of the network access requester, as well as the integrity state of the platform.

b) Authorize the terminal strategy: to establish a credible end-state level, such as: confirm the existence of application, status, upgrades, upgrade anti-virus software and IDS rule base version, terminal operating system and applications patch level, etc. So that the terminal is given a network login permission policies so as to obtain the certain rights under the control of access to the network.

c) Access Policy: Make sure the terminal machine and its user privileges, and establish credibility level before connection the network, balance the existing standards, products and technology.

d) Assessment, quarantine and remediation: Ensure the terminal which does not meet the needs of the credible strategy outside the trusted network, if possible, perform appropriate remedial measures.

2) TNC infrastructure.

The TNC infrastructure is shown in Fig. 3, include three entities, three levels and a number of interface components [13]. The architecture increase integrity measurement layer and integrity assessment layer in the traditional network access layer, to achieve the access platform authentication and integrity verification.

Three entities are the access requester (AR), the Policy Enforcement Point (PEP) and policy decision points (PDP). AR issue the access request, collect the integrity trusted information of platform, sent to the PDP, apply for a network connection; PDP make decisions AR access request according to local security policy, the determine basis include the AR platform identity and integrity of the state of AR, the judging result is enable / disable / isolation; PEP control the access to the protected network, implement access control decisions of PDP.

AR include three components: network access requester (NAR) issue the access request, apply for a network connection, in an AR can have more than one NAR; TNC Client (TNCC) collect the integrity measurement information from integrity measurement collector (IMC), and measure and report the integrity information of platform and IMC; IMC measure the integrity of the various components of the AR, in an AR can have a number of different IMC.

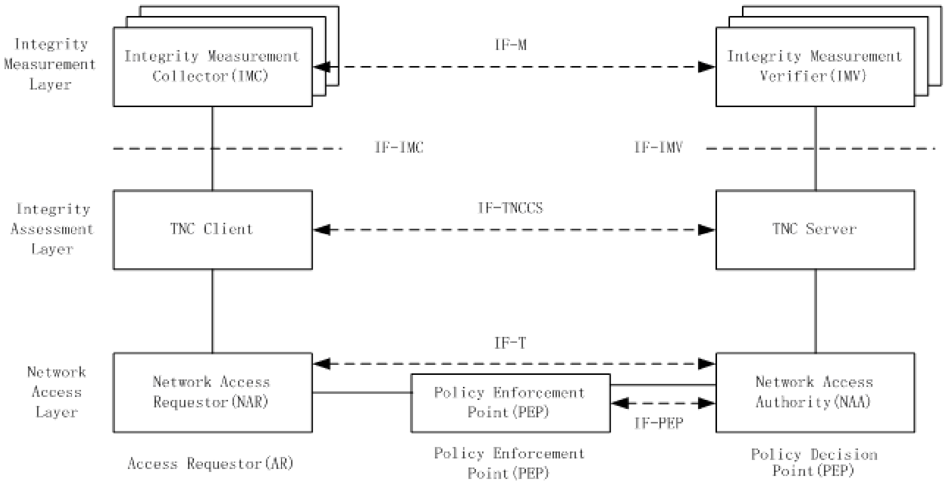
Integrity Measurement Layer
Integrity Measurement Collector(IMC)
IF-M
Integrity Measurement Verifier(IMV)
IF-IMC
IF-IMV
Integrity Assessment Layer
TNC Client
IF-TNCCS
TNC Server
IF-T
Network Access Layer
Network Access Requestor(NAR)
Policy Enforcement Point(PEP)
Network Access Authority(NAA)
IF-PEP
Access Requestor(AR)
Policy Enforcement Point(PEP)
Policy Decision Point(PEP)

Fig. 3. TNC infrastructure.

PDP include three components: network access authority (NAA) make decisions on the AR network access request [14]. NAA can consult the top of the trusted network connection server (TNCS) to determine whether the integrity state of AR is consistent with the security policy of PDP or not, to determine whether AR's access request is allowed; TNCS responsible communication between TNCC, collect decision form integrity measurement verifier (IMV), form a global access policy passed to the NAA; IMV verify the integrity measurement information of the various components of AR passed by IMC, and give advice for access to decision-making.

Three levels are the network access layer, integrity assessment layer and integrity measurement layer. Network access layer support traditional network connection technologies such as 802.1X and VPN mechanisms. Assessment layer authenticate the platform, and assess the integrity of AR. integrity measurement layer collect and verify the integrity-related information of AR.

In the TNC architecture there are multiple entities, in order to achieve interoperability between the entities, needed to develop an interface between the entities [15]. Interface bottom-up including IF-PEP, IF-T, IF-TNCCS, IF-IMC, IF-IMV and IF-M. IF-PEP is the interface between PDP and PEP, maintain transmission information between PDP and PEP; IF-T maintain transmission information between AR and PDP, and provides the package for the upper layer interface protocol, and specification for EAP methods and TLS were developed; IF-TNCCS is the interface between TNCC and TNCS, defines the protocol of transmission information between TNCC and TNCS; IF-IMC is the interface between TNCC and the various components of IMC, and defines the protocol of transmission information between TNCC and IMC; IF-IMV is the interface between TNCS and the various components of IMV, and defines the protocol of transmission information between TNCS and IMV; IF-M is the interface between IMC and IMV, and defines the protocol of transmission information between IMC and IMV.

3) TNC basic process

The version of TNC1.4 as an example, a full TNC basic process is shown in Fig. 4.

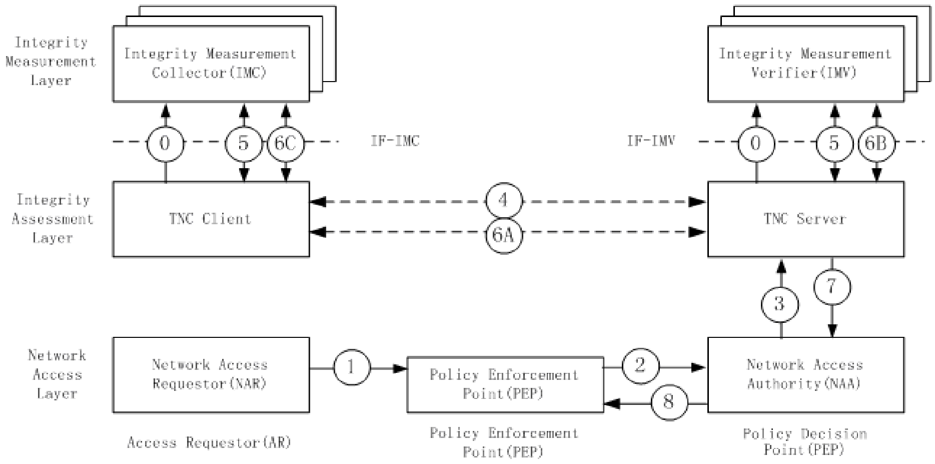
Integrity Measurement Layer
Integrity Measurement Collector(IMC)
Integrity Measurement Verifier(IMV)
0
5
6C
IF-IMC
IF-IMV
0
5
6B
Integrity Assessment Layer
TNC Client
4
6A
TNC Server
3
7
Network Access Layer
Network Access Requestor(NAR)
1
Policy Enforcement Point(PEP)
2
8
Network Access Authority(NAA)
Access Requestor(AR)
Policy Enforcement Point(PEP)
Policy Decision Point(PEP)

Fig. 4. TNC process.

Step 0: Before connecting the network and verifying platform integrity, TNCC need to initialize each IMC. Similarly, TNCS must initialize the IMV.

Step 1: When the network connection request occurs, NAR sends a connection request to the PEP.

Step 2: After receive NAR access request, PEP sent a network access decision request to NAA. Assume that NAA has been set the order to operate in accordance with user authentication, platform authentication and integrity check. If there is an authentication fails, and then the certification will not occur. User authentication can occur between the NAA and AR. Platform authentication and integrity check occur between AR and TNCS.

Step 3: Assume that user authentication between AR and NAA is completed successfully, then NAA notice TNCS that a connection arrives.

Step 4: TNCS and TNCC is being platform verification.

Step 5: Assume that platform verification between TNCC and TNCS is completed successfully. TNCS IMV that new connection request has occurred, need for integrity verification. At the same time TNCC notice IMC that a new connection request has occurred, the integrity of information need to be prepared. IMC through IF-IMC to TNCC return IF-M messages.

Step 6A: TNCC and TNCS exchange information related to integrity verification. This information will be forward by NAR, PEP and NAA, until the integrity state of AR meet the requirements of TNCS.

Step 6B: TNCS sent each IMC message to the corresponding IMV. IMV analysis the IMC information. If IMV need more integrity information, it will be through IF-IMV interface to send a message to TNCS. If IMV has been determined the integrity of information of IMC, it will through IF-IMV interface to send the result to TNCS.

Step 6C: TNCC forward information from TNCS to the appropriate IMC, and forward information from IMC to TNCS.

Step 7: When TNCS has completed the handshake with TNCC integrity check, it sends TNCS recommended actions to the NAA.

Step 8: NAA send network access decisions to the PEP to implement. NAA must also explain TNCS the last network access decisions, this decision will also be sent to the TNCC. PEP implement decisions of NAA, the network connection process is completed in this time.

The above process does not include the case that integrity verification did not pass. If the integrity verification is not passed, AR can access PRR through PRA, update and repair the relevant components, and then repeat the above process. Update and repair process may be repeated several times until the integrity verification passed.

4) TNC support technology

Although TNC integrity measurement and reporting is the core technology, but TNC architecture use some of the existing technology to provide support for the top of trusted computer system. This includes network access technology, secure messaging technologies and user authentication technology.

TNC network access layer based on existing network access technologies, include 802.1X, virtual private network (VPN) and point to point protocol (PPP). 802.1X provides access control based on port for LAN, can through controlled port and uncontrolled port to control the network connection, it is currently the most widely used application of network access methods [16]. VPN uses the internet key exchange (IKE) protocol and IPsec protocols, SSL or transport layer security (TLS) to establish a secure tunnel on the Internet to ensure the security of data transmission. PPP protocol provides standard method of transmitting a variety of protocol datagram in point to point connection.

TNC architecture needs to pass message between entities of multiple components, so the security messaging technology is also key. Extensible authentication protocol (EAP) is widely used in 802.1X framework. EAP can not only transmit authentication information, but also pass terminal integrity measurement information through EAP method. HTTP protocol and HTTPS is used to transport application-related information. TLS can pass the integrity reports and shake hands with the news of integrity check.

In the user authentication of network access control, TNC does not enforced use any protocol, but can use existing RADIUS protocol and Diameter protocol.

Can be seen in the trusted network connect architecture; the underlying network access layer basically follows the existing network access control technology, especially the authentication protocol. Message transmission also uses the existing norms; makes the trusted network connect architecture easy compatibility with existing network access systems.

3.4. UAC Technology

UAC is a universal access control solution proposed by Juniper company, UAC consists of several modules, including the infranet controller as centralized policy manager, client agent software UAC (For client which do not support downloadable, such as external staff equipment, use gentles mode) and a variety of different forms of enforcement points, including the Juniper firewall and switch which support third-party 802.1X protocol or wireless access points.

a) Infranet controller: Infranet Controller is the core component of UAC. The main function of UAC is to apply UAC proxy to the user's terminal computer, in order to collect user authentication, endpoint security state and device location information or collect the same information in agent-less mode, and combine this information and strategies to control the network, resource and application access [17]. Subsequently, Infranet controller passes 802. IX at the network edge before IP address assigned, or in the network core pass the strategy to the UAC enforcement points through the firewall.

b) UAC Agent: UAC agent deployed on the client, which allows dynamic download. The host checker function which UAC agent provide allows administrators to scan endpoint and understand the variety of security applications or states, including but not limited to anti-virus, anti-malicious software and personal firewall. UAC agent can assess the security status of the latest definition through the pre-defined host check strategies and automatically monitoring function of anti-virus signature files. UAC agent also allows custom inspection tasks, such as check registry and port status, and can perform an MD5 checksum to verify whether the application effective.

c) UAC enforcement points: UAC enforcement points include 802.1X switch / wireless access point, or the Juniper networks firewall / VPN platform.

4. Compare and Analysis

Based on the above analysis we can see, the goals and implementation techniques of NAC, NAP, UAC and TNC technology have great similarities:

First, they object is to ensure the host safety access, that is, when PC or laptop access to the local network, through its special protocol verification, in addition to verify user identity information such as user name, password, user certificate, but also verify whether the terminal meet security policy administrator developed or not, such as operating system patches, virus database version and other information. And each developed their own isolation strategy, through access devices (firewalls, switches, routers, etc.); force the terminal equipment which dose not meet the requirements isolated in a designated area, only allowed access to the patch server to download updates. In the end hosts do not verify the safety issues, and then allow it to access the protected network.

The individual keys for nodes and Sink shared key, the node through the main key pre distribution and pseudorandom function before deployment to generate. If two adjacent nodes are to generate the key pair, then through the exchange of the identifier and the master key pre distribution and one-way hash functions to calculate. If the node as cluster head to establish shared with its neighbor node cluster key, then generate a random key as the cluster key, and then use and neighbor node matching keys one by one team cluster key encryption sends the corresponding node, the neighbor node saves the decryption of the cluster key down, communication secret group key for Sink and all nodes sharing.

In this paper, using Sink as the trusted key distribution center network establishing pair wise keys and the broadcast packet authentication for network node. The SPINS protocol consists of two parts: SNEP (secure network encryption protocol) and TESLA (timed efficient stream loss-tolerant μ authentication) data confidentiality and authentication of. SNEP to realize the data mainly through the use of a counter, and it is a message authentication code mechanism. Communication between the key and MAC key pair through the master key and pseudo random function to generate use obtained from Sink. SNEP makes the protocol to the semantic level of security, to ensure the fresh data; MAC key length is fixed, only 8 bytes, not to increase too much communication load.

This paper provides the authentication mechanism effectively. Key negotiation need data packets and the node identity for effective certificate, otherwise cannot guarantee the correctness of communication key set, MAC mechanism in the symmetric key pipe is forged the problems, based on the digital signature mechanism of non symmetric key is not applicable to WSN, provides the authentication mechanism in accordance with WSN characteristics it is important to research the key management. Intrusion tolerance and fault tolerance support. Node "vulnerable and calculation of communication ability is limited, so that nodes are vulnerable to DoS, comprehensive defense DoS attack is more difficult.

Second, the implementations of these techniques are relatively similar, are divided into three main levels: client, policy services, and access control.

On the other hand, due to the release own background of the four technologies, the four technologies existence different emphasis. Because NAC is released by Cisco, so access equipment in its structure accounted for a large proportion, or NAC itself is a device designed around Cisco, UAC and Cisco are similar, but also design around Juniper's equipment, but follow this standard protocol such as 802.IX in the access service choice side. NAP agent emphasis in the terminal agent and access (VPN, DHCP, 802.1x, IPSec components) service, this have great relevance with Microsoft's own technical background; TNC technology emphasis in verifying the identity of the host bound with TPM authentication and integrity verification, or TCG aims to provide application support to TPM released by TNC.

From development, at present NAC and NAP have been allied, network access device is using Cisco's NAC technology, and host client is using Microsoft's NAP technology ,to achieve two complementary situation, benefit to the further development. However, several vendors have launched their own way in the network access and control standards, the standards war need to wait a long time. In any case, we see that the future network security transform from the threat defense to security design, security will be built into our network technology, the network is safe from the start, and network access control technology is a step in this direction.

References

[1]. Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang, Research on trusted network connection, *Chinese Journal of Computers*, Vol. 33, No. 4, 2010, pp. 707-717.

[2]. Zhang Feng-Sheng, Concentration design and implementation of NAC system, *Financial Computer of China*, No. 2, 2006, pp. 48-50.

[3]. Li Wen-Jing, Network access control – NAC, *China Internet*, No. 11, 2005, pp. 31-32.

[4]. Qi Qing-Hua, Past and present of NAP technology, *Software World*, No. 6, 2008, pp. 63-65.

[5]. Lu Lai-Zhi, Gao Zhong-He, Thinking of security problems of NAP-PT protocol conversion, *Computer Knowledge and Technology*, No. 11, 2008, pp. 227–231.

[6]. Wang Jing-Yu, Tan Yue-Sheng, Self-defense system based on 802.1X and Web technology, *Computer & Digital Engineering*, Vol. 38, No. 8, 2010, pp. 52-54.

[7]. Lu Zhi-Pei, Yao Guo-Xiang, Luo Wei-Qi, Design and implementation of NAC model based on 802.1x, *Computer Engineering*, Vol. 36, No. 4, 2010, pp. 147-149.

[8]. Wang Xiao-Jun, Network access management – Windows Server 2008 NAP, *China Internet Week*, No. 11, 2008, pp. 113.

[9]. Lu Hai, Application and analysis of network access control, *Information and Electronic Engineering*, Vol. 7, No. 10, 2009, pp. 483-487.

[10]. Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang, Research on trusted network connection, *Chinese Journal of Computers*, Vol. 33, No. 4, 2010, pp. 707-717.

[11]. He Xin, New generation of network security access technology-TNC, *Information Network Security*, No. 3, 2007, pp. 71-73.

[12]. Chi Ya-Ping, Yang Lei, Li Zhao-Bin, Fang Yong, Design and implementation of an authentication scheme for trusted network connection based on EAP-TLS, *Computer Engineering & Science*, Vol. 33, No. 4, 2011, pp. 8-12.

[13]. Han Li, Xie Qiang, Design and implement on security access control system based on TNC, *Microcomputer Information*, Vol. 26, No. 1-3, 2010, pp. 74-75.

[14]. Zhu Xiao-Dong, Gao Feng, Hu Hai-Zhou, UAC mechanism inside Windows 7 and its security analysis, *Computer Engineering and Design*, Vol. 24, No. 31, 2010, pp. 5172-5191.

[15]. Li Xue-Feng, Xu Kai-Yong, Applying UAC in Windows XP and its implementation, *Computer Applications and Software*, Vol. 26, No. 3, 2009, pp. 265-267.

[16]. Yan Fei, Ren Jiang-Chun, Dai Kui, Wang Zhiying, Design and implementation of security authentication protocol based on TNC, *Computer Engineering*, Vol. 33, No. 12, 2008, pp. 162-165.

[17]. Chen Jiang, Peng Xin-Guang, Analysis of network access control technologies and their comparative, *Computer Development & Applications*, Vol. 24, No. 5, 2011, pp. 6-8.

___