Heterogeneous Wireless Network Security Architecture
draft-huang-wireless-security-architecture-00

ABSTRACT

After analysis and comparison of domestic and international wireless network secure schemes and standards, security threats for heterogeneous wireless network are investigated in theory and practice. According to the comprehensive summing-up of current secure standards’ application, existing secure vulnerabilities and secure hidden troubles which may happen in future, "network layered, security classified and trusted domain departed" secure standard model is proposed, and corresponding standards for heterogeneous wireless network security architecture are also put forward.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 1, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1. Introduction..................................................4
  1.1. Requirements............................................4
  1.2. Terminology.............................................4
  1.3. Purpose................................................5
2. Security standards for wireless broadband networks Analysis..5
  2.1. Security Standards for Wireless LAN (WLAN)..............6
  2.2. Security Standards for Wireless MAN (WMAN)..............6
  2.3. Security Standards for Wireless WAN (WWAN)..............7
  2.4. Heterogeneous Network Access Authentication Mechanisms..8
     2.4.1. UMTS–WLAN Authentication Mechanism.............8
     2.4.2. Integration Architecture for WiMAX–3G...........9
  2.5. Future Development of Access Security Standard........10
3. Security Analysis of Wireless Broadband Network Standards....11
  3.1. Security Analysis of Existing Standards...............11
     3.1.1. Security Analysis of WEP........................11
     3.1.2. Security Analysis of WPA1........................13
     3.1.3. Security Analysis of WAP2........................14
     3.1.4. Security Analysis of WAPI.........................15
  3.2. Security Analysis of Some Key Technologies............16
     3.2.1. Security Analysis of TKIP........................16
     3.2.2. Security Analysis of EAP........................16
     3.2.3. Security Analysis of LEAP.........................17
     3.2.4 Security Analysis of PAP............................18
     3.2.5. Security Analysis of PEAP.........................20
4. Wireless Broadband Network Security Architecture............21
  4.1. Framework model........................................21
     4.1.1. Security Classification..........................22
     4.1.2. Security Domain....................................23
  4.2. System Framework Content................................23
     4.2.1. Heterogeneous Network Access Security Technology...24
     4.2.2. Password Security Technology......................25
     4.2.3. Mobile Terminal Secure Technology................26
     4.2.4. Access Control Technology.........................27
     4.2.5. Wireless Intrusion Detection Technology..........30
     4.2.6. Mobile E-commerce secure technology............32
5. IANA Considerations..........................................33
6. Security Considerations.......................................34
7. References................................................................34
  7.1. Normative References....................................34
Author’s Address..................................................34
1. Introduction

Heterogeneous wireless network is expected to provide mobile users with freedom of roaming between diverse set of wireless networks, since different wireless networks have different security standards and requirements, mobile terminal should hold various secure schemes. This document considers the security mechanisms in heterogeneous wireless networks, such as secure system architecture.

This document defines "network layered, security classified and trusted domain departed" secure system model, which proposes several secure technologies (such as access secure technology, password secure technology, mobile terminal secure technologies and so on) to meet different service requirements.

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Terminology

This document frequently uses the following terms:

Heterogeneous wireless network

Heterogeneous wireless network is the trend of next-generation network; it refers to different network based on different low layer technologies integrate as a whole, so user can really achieve the goal that anyone can communicate with anybody in anywhere when anytime.

Wireless broadband networks

Wireless broadband networks refers to networks which can provide more efficient services for different people and different needs, and also provided ways to achieve mobility, personalization of communication and multimedia applications. WLAN, WiMAX and 3G are the typical Wireless broadband networks.

Security Standards

Authentication, access control scheme and encryption technologies are part of secure technologies, if they are employed by some networks, they become security standards of these work, such as PKM for WiMAX.
Security Analysis

Security schemes are analyzed via contrasting others and linking them to the reality application. Through security analysis, advantages and disadvantages of protocol or scheme can be found thoroughly.

Security Architecture

Security architecture in this document is "network layered, security classified and trusted domain departed" secure system frame.

1.3. Purpose

One purpose of this document is to provide a fundamental security investigation of security in heterogeneous wireless networks. The other one is to offer a reference for researchers who would study this field.

2. Security standards for wireless broadband networks Analysis

Multiple heterogeneous wireless networks will be coexistence for a long time in next-generation broadband wireless communication network of (WLAN, WiMAX, etc.). A variety of network access technologies, such as: TD-SCDMA, WCDMA, cdma2000 for wireless wide area network, WiMAX for wireless metropolitan area network and Wi-Fi for WLAN technology, provided more efficient services for different people and different needs, and also provided ways to achieve mobility, personalization of communication and multimedia applications. At the same time, on a variety of wireless network performance, especially security requirements put forward higher requirements, so specialized security protection mechanisms are in need. The access users should perform authentication and access control to protect the confidentiality and integrity of transmission data. However, wireless broadband network security cannot be satisfied in the whole because of independent and incompatible of different wireless network security standards. Therefore, heterogeneous wireless network security architecture standards need to be developed.

By tracking security standards of domestic and international wireless network, Analysis and comparison of various security mechanisms of wireless networks are presented. Security threats that wireless network may suffered are concluded and summarized in theory and practice. This architecture exploited the usability of security protocols and encryption algorithms in wireless network
from throughput, security, fault tolerance, balance between efficiency and other aspects, and estimated the anti-attack capability of information security systems (including encryption algorithms, security protocols and key management, etc.). A brief description of existing wireless broadband network standards in the literature will be presented.

2.1. Security Standards for Wireless LAN (WLAN)

Design of WLAN standard starts early and goes on a long term. It has become a mature international standard, and has a wide range of applications, including IEEE802.11 (WEP), IEEE802.11i and WPA and WAPI. IEEE 802.11 standard achieved authentication and data encryption through WEP (Wired Equivalent Privacy). IEEE 802.11i which is published by IEEE802.11 Working Group in June 2004 is to enhance the security of WLAN further and ensure compatibility of wireless security technology between different manufacturers. IEEE 802.11i defines a robust security network (RSN) of Key Management Protocol based on 802.1x Wi-Fi alliance formulates WPA standard as a transition. WPA uses 802.1x and TKIP to implement WLAN access control, key management and data encryption. WAPI which has independent intellectual property is standards for wireless network technology in China. WAPI uses Elliptic Curve Cryptography algorithm within public key cryptosystem and block cipher system of secret key approved by State Encryption Administration Commission, to achieve device authentication, link authentication, access control and encryption to protect user information under wireless transmission. It will completely change the current situation with a variety of security mechanisms co-exist and incompatible for WLAN.

From the above description, it seems that areas covered by international standards are mainly on user and network authentication, key exchanging, access control and data encryption. However, user security in the heterogeneous wireless network has not involved, which is also suitable for end-to-end security framework in cross-domain environment.

2.2. Security Standards for Wireless MAN (WMAN)

WMAN (WiMAX) security standards mainly include 802.16 D3, 802.16E and South Korea’s WiBro. 802.16 D3 defines a secure sub-layer on MAC layer to guarantee security. Secure sub-layer consists of two protocols: Data Encryption Encapsulation Protocol and Key Management Protocol (PKM). Data Encryption Encapsulation Protocol defines encryption suite supported by IEEE 802.16 protocol, which includes data encryption and integrity verification algorithm,
and rules of applying these algorithms to MAC PDU load. Key management protocol defines secure distribution way of key data from base station to user workstation and key data synchronization and restrictions to access network services. 802.16e is enhanced based on the 802.16d to support vehicular and mobile services between 2–11GHz band, and support handoff between station and sector. It is mainly to solve some existing deficiencies of original 802.16 security mechanism. IEEE 802.16e secure sub-layer supports PKMv1 and PKMv2 two versions. PKMv2 can support broadcast and multicast service, MSS and BS mutual authentication, etc.

Standards of WiBro (Wireless Broadband) is beginning in January 2004, which is developed from the Electronics and Telecommunications Association (ETRI), Samsung Electronics and HPI (High Speed Portable Internet) project launched by South Korea’s major operator. South Korea’s Ministry of Information and Communication declared definitely that WiBro should fully comply with 802.16e and began to coordinate with 802.16e to integrate WiBro and 802.16e.

2.3. Security Standards for Wireless WAN (WWAN)

TD-SCDMA, WCDMA and cdma2000 are the major communication specification of 3G system, and they have comprehensive security mechanisms. With inherit of the advantages of 2G system, comprehensive security features and security services are defined based on the new features of 3G. Security mechanisms of 3G system mainly include 3GPP and 3GPP2. 3GPP and 3GPP2 have corresponding security standards respectively for service, including WAP security, presence service security, location service security, mobile payment services security, filtering mechanisms for spam short messages and DRM standard to prevent reproduction without authorized and so on.

Mobile Internet terminals have identity authentication function and have access control function for various system resource and services application. Security of identity authentication can be realized through password or smart card and entity identify mechanisms. Security protection and access control for data service can be realized through policy of access control. For data stored in the terminal, hierarchical storage and data integrity check and other means can be used to ensure security.

In addition, with greatly increasing applications of mobile IP, how can authentication systems support user roaming and across administrative domains authentication become the current research focus. Diameter which developed from RADIUS has better scalability. AAA Working Group of Internet Engineering Task Force (IETF)
developed a mobile IP (MIP) AAA standard based on the Diameter protocol. Solutions extend the AAA function through the access router of mobile IP network, realize mobile node access control, and support mobile IP fast handoff.

2.4. Heterogeneous Network Access Authentication Mechanisms

The integration of heterogeneous wireless networks may be inevitable in the future development of B3G/4G. Recently, Integration architecture and related technologies for implementation of heterogeneous wireless networks become the focus among information technology companies and academe researchers. Many countries and specification organizations have already set up working groups for the study of integration of heterogeneous networks and related technologies. However, implementation of integrated network is a complex and large project. Integration architecture with design comprehensive and good scalability is few. The major integrated architectures proposed realized it through simple interworking between two or more heterogeneous networks, such as 3G-WLAN interworking, 3G-WiMAX interworking, and CDMA2000-WLAN interworking, etc. Implementation of integrated network requires the support of various key technologies, and the security mechanism is the key for successful application of integrated network. Access authentication mechanisms regard as the first step of security. Different access technologies have different ways to guarantee different access authentication. How to design a universal access authentication mechanism which can provide seamless secure roam and enjoy services for mobile user in the wireless networks is a major technical challenge for integration network.

2.4.1. UMTS-WLAN Authentication Mechanism

According to the difference of interconnected location, the implementation approaches can be classified several kinds as following:

Interworking architecture based on MIP (Mobile IP): The architecture takes 3G and WLAN as two kinds of peer networks which are connected through internet and the MIP can be achieved through the home-agent (HA) and foreign-agent (FA) set in the network. The GGSN (GPRS Gateway Support Node) in the home network of 3G is set as HA, and SGSN (Serving GPRS Support Node) in the foreign network of 3G is set as FA. HA in WLAN is located in DNS (Domain Name Server), while FA is located in the DHCP (Dynamic Host Configuration Protocol) server.
Interworking architecture based on inter-connection gateway: The architecture also takes 3G and WLAN as two kinds of peer networks while a inter-connection gateway is added. The mobile nodes perform mobility management in the 3G network according to the 3G network’s session management and the GPRS mobility management, while in WLAN covering areas with hot spots executes the WLAN mobility management mechanism. Such kind of integration plan can simultaneously provide services to both single-mode user and dual-mode user. Mobility management of dual-mode user can exchange signal through gateway.

Tight Coupling Architecture: this architecture takes the WLAN network as one of the access network of 3G Core Network (CN), which satisfies the interworking requirements for WLAN access to the packet domain traffic of 3G network, such as allowing WLAN to access, for access control and accounting based on 3GPP system, and for unified accounting and customer services, service continuity.

Loose Coupling Architecture: This architecture separates logically 3G service domain and WLAN service domain. Location management and authentication, authorization, accounting in the handoff process between WLAN and 3G network can be realized through MIP, so the WLAN standard has the fewest changes.

Semi-tight Coupling Architecture: WLAN and UMTS can be working concurrently in this architecture, but the major signaling for interconnection (i.e. authentication messages with user identifier) is carried over UMTS access network and core network to the WLAN. Signaling which cannot be carried through UMTS is still carried over WLAN. If the Hybrid-authentication is successful, traffic can also be carried over WLAN.

2.4.2. Integration Architecture for WiMAX-3G

According to the tightness, the architecture for integrating 3G system and WiMAX can be categorized into loose coupling and tight coupling architecture. The interworking has six common scenarios: (1) Common Billing and Customer Care; (2) 3G system based Network Authentication and Accounting; (3) WiMAX Access to 3G system Packet-Switched based services; (4) WiMAX Access to 3G system Packet-Switched based Services with Service Consistency and Continuity; (5) WiMAX Access to 3G system Packet-Switched based Services with Seamless Service Continuity; (7) WiMAX Access to 3G system Circuit-Switched based Services.

The first two scenarios belong to the loose coupling mode, and the latter four scenarios belong to tight coupling mode. In
scenario (1), there is a network appended between two systems in which AAA is located to accomplish authentication and accounting; In scenario (2), as the complementary network of 3G system, authentication and accounting of WiMAX should use Home Location Register (HLR), AAA etc. of 3G system, while traffic export of WiMAX directly connects to MAN; In scenario (3), Authentication and accounting in WiMAX is just like scenario (2), and packet domain gateway of 3G system takes responsibility of its traffic export; In scenario (4), WiMAX can directly access all services of 3G system; In scenario (5), WiMAX network handoff should be controlled by 3G system and its VoIP service can handover to 3G system; In scenario (6), radio resources of WiMAX and 3G system will be schedule centralized.

Authentication and accounting of WiMAX terminals are implemented in the corresponding entities of 3G system. Under the loose coupling scenario, WiMAX proprietary equipments achieve mobility management of WiMAX, while equipment in 3G system should participate in mobility management of WiMAX terminal under the tight coupling scenario. WiMAX may firstly consider adopting scenario (1), then through the updates of 3G system it can evolve gradually to scenario (4) and (5) and achieve ultimate target of evolution scenario (6).

2.5. Future Development of Access Security Standard

From the above descriptions of the wireless broadband security standards, the access security issue using the same communication technology has been basically solved, with the relatively mature security mechanism and safety standards accepted by the industry on the whole. However, new security issues appeared with the changes of emerging markets demand and network technology evolution. Driven by the objective demands of resource sharing, information integration, supply chain construction etc., large-scale resource sharing mode makes the work flow and sensitive data processing facing unprecedented security threats, while the existing international security standards cannot meet the security needs of heterogeneous networks. Some areas of security have appeared yet these international standards have not mentioned, and the problem of heterogeneous network access security has placed in front of network integration and market expansion. Heterogeneous network security standard is still in its infancy internationally, the domestic work in this area still stays only in academic research.

According to wireless communication industrial distribution of our country, mobile communication technology (3G) will hold a dominant position, and other technologies (WLAN, WiMAX) will be considered
as auxiliary technologies. This multi-mode communication distribution will provide many kinds of services. Because of coexistence of heterogeneous networks, roaming and domain crossing will become more common and complex in the next-generation broadband wireless mobile communication network, and high level privacy protection is taken more attention when user accessing network. It is a common viewpoint for international standard organization that the problem of roaming secure access can be solved via using public key cryptography. There are many authentication and key exchange protocols and patent technologies, but they can meet the certifiable secure requirements under the domain crossing condition. Furthermore, there are few of certifiable secure protocol which can provide high level privacy protection when crossing different domains. Therefore, it is practical and valuable to investigate and propose corresponding specifications which meet the secure requirements when roaming within mobile networks.

3. Security Analysis of Wireless Broadband Network Standards

The rapid development of network technology has impacted and influenced network security, and with the diversity of network attack techniques safety standards (protocols) analysis and attack tools are becoming increasingly various. The original safety standards become unsafe or there are obvious security risks.

3.1. Security Analysis of Existing Standards

3.1.1. Security Analysis of WEP

The purpose of WEP is to ensure confidentiality, integrity and authentication in the wireless communication environment and to provide equivalent privacy as wired environment. WEP uses RC4 stream cipher algorithm to encrypt data, and the CRC (Cyclic Redundancy Check) as the data integrity check algorithm. Encryption key used is 40 bits with a 24 bits initial vector IV as auxiliary encryption input. Initially 802.11 WEP Protocol Working Group just designed a protocol under wireless environment with little considerations of security. WEP security problems exist mainly in the following areas:

(1) WEP cannot resist exhaustive key search: 40 bits key is too short to meet the security needs. Although you can use longer keys, it easily leads to re-use keys for the small scope of the initial vector and the adversary can still decrypt the message.

(2) All users of the network use the same authentication key, so
it doesn’t actually achieve authentication. The valid users of the network can pretend other users to send messages.

(3) CRC integrity verification algorithm can detect changes on the messages, but without hash function an attacker can forge messages at will. Obviously, CRC is not cryptographic secure.

(4) Keys of different users are not independent of the MAC addresses.

(5) Without description of production for the initial vector IV, different IVs are prone to collide which leads to key exposure. 802.11 Working Group recommends that different data packets uses different initial vectors, but the range is small so that it is easy to collide.

(6) It is difficult for key re-distribution when deleting a user of the authorized list.

(7) Using the RC4 stream cipher algorithm itself is not secure and there have been attacks of RC4.

(8) There are no measures against replay attacks.

For RC4 encryption system, the specific attacks of the WEP protocol are:

(1) FMS attack (2001): FMS attack is the first key recovery attack, and the principle is based on the predictable head. The attacker first obtains some front bits of the key stream, resulting in correlation with the other bits. Under the FMS attack, the probability of a successful attack more than 50% may need 4 to 6 million packets.

(2) Korek attack (2004): Based on the FMS attack, but the relevance of RC4 key stream increases. The probability of a successful attack more than 50% may take only about 70 000 packets.

(3) PTW attack (2007): Expanding the FMS attack and Korek attack, each packet is processed to detect the correctness of the key. The probability of a successful attack more than 50% may take only 35 000 to 40 000 packets.

(4) Chopchop attacks: Allow an attacker to send 128*m packets in order to decrypt the last m bits, but the attack will not lead to disclosure of the root key.
3.1.2. Security Analysis of WPA1

Although WEP basically doesn’t achieve any security goals, but practically many devices support WEP protocol. Given urgent market demand to improve the security of WLAN, Wi-Fi alliance formulates WPA standard as a transition. WPA uses 802.1x and TKIP to implement WLAN access control, key management and data encryption. 802.1x is a port-based access control standard, users must pass authentication and authorization and then access network resources through the port. Although TKIP is based on RC4 encryption algorithm as WEP, it introduces four new algorithms:

* Extended 48-bit initial vector (IV) and IV Sequencing Rules
* Per-packet key construction
* Message Integrity Code (MIC)
* Key to re-access and distribution mechanism

WPA adds a Key Mixing Function, ensuring the independence between the key of different data packets by the expansion of Initial Vector Space, and also using Michael algorithms to improve data integrity. Although TKIP adds Key Mixing Function, and has been greatly improved in security, however, it is not as safe as expected. We can find the MIC key through a data packet key, if we continue the use of short-term key TK, and the same initial vector, then the security of the entire system will be destroyed. This defect is not to say TKIP unsafe, but some parts of the TKIP unsafe. There are some attacks to WPA:

(1) In 2004, some scholars have found that by using a given number of RC4 data packets encryption key, an attacker may get short-term key TK and message integrity check key MIC. This attack is not an actual attack, but can reduce the restore complexity of the key TK from 2128 of the Infinite Search to 2105. This attack shows that the security of WPA depends on the key of all the data packets.

(2) Off-line dictionary attack: As the master key of WPA is generated by the Passphrase and SSID, and the session key is generated by the master key, the user’s MAC address, the user’s random number and random number of access point AP, then the attacker only needs to get SSID, MAC address, and random numbers to obtain Passphrase by off-line dictionary attacks.

(3) In November 2008, researchers found a way to crack WAP, and even to complete it within 15 minutes. However, this method only applies to Wi-Fi adapter’s data, and it does not work for the encrypted...
data from the PC to the router. When TKIP encryption system is being cracked by the Bulk Data Algorithm, the security is greatly reduced, however, this attack is different from original methods. When the implementation of this attack, a lot of data from WPA router has been used, and can finally break encryption system by combining with an algorithm. Some elements of this method have been incorporated into Aircrack-ng Wi-Fi encryption hacking tool system, which is primarily used by system intrusion tester and other officers. Viewing that the WEP and WPA encryption are not so secure, experts recommend WPA2 for wireless network system.

### 3.1.3. Security Analysis of WAP2

To make up the security of WEP protocol, Wi-Fi Alliance used WPA1 as a transitional security standard, and designed WPA2 as the ultimate standard of wireless network security. WPA2 uses the same authentication process, 4 rounds handshaking, and layered keys with the WPA1. However, it uses AES to replace TKIP, uses AES counter encryption mode and uses CBC mode of AES as the data integrity verification. WPA2 has two versions, one is WPA2 Enterprise version, mainly using 802.1x and EAP method for certification; and the other is WPA2 Home version, using(pre-shared-key)PSK-based authentication, and do not need RADIUS. The improvements of WPA2 in security are:

1. **WPA2 authentication**: WPA2 requires authentication with two stages, first open system authentication, and then 802.1x and EAP methods authentication. For the network without RADIUS (Remote Authentication Dial-In User Service) infrastructure, such as small office and home networks, WPA2 also supports the use of PSK (pre-shared key).

2. **WPA2 key management**: the same with WPA, WPA2 requires a PMK (primary master key) generated through the EAP or PSK authentication processes and calculate TK (temporary key) by 4 rounds hand-shaking.

3. **Using AES**: WPA2 required equipment to support AES encryption using Counter-mode, and support AES data integrity verification of CBC mode (CCMP). AES encryption system can attain the U.S. national standard safety requirements.

4. **WPA2 supports for fast roaming.**

5. **WPA2 is compatible with WPA and WEP**, besides WPA2 devices can also support WPA and WEP. Compared with WPA, the security of WPA2 has been greatly improved. Nowadays, the major attack is Off-line Dictionary Attack, which is the same with the attack in WPA.
However, the effect of this attack is not so good. WPA2 encryption use AES instead of RC4, so it has been the most secure wireless security standard.

3.1.4. Security Analysis of WAPI

In addition to the international standard IEEE 802.11i and WPA security, the national standard for wireless local area network GB15629.11 is also proposed in China, which is the only approved protocol in China in this field. The standard includes a new WAPI security mechanism, which is made up of WAI (WLAN Authentication Infrastructure) and WPI (WLAN Privacy Infrastructure) two parts, used to identify the user and encrypt the transmission data. WAPI can provide comprehensive security protection for users’ WLAN system. WAPI security mechanism includes two components.

By means of public key cryptography, WAI also uses certificates on authentication of STA and AP in WLAN system. WAI defines an entity named ASU (Authentication Service Unit), in order to manage the certificates required by all parties of information exchange (including certificate generation, issuance, revocation and renewal). Certificates which contain the public key and signatures of the certificate issuer (ASU) and the certificate holder (the signatures here use unique WAPI elliptic curve digital signature algorithm), is the digital credentials of network equipment. In the specific implementation, the authentications for each other are needed after STA associated to the AP. Firstly, STA will submit its own certificate and current time to AP, then AP uses STA’s certificate, current time and its own certificate to format signature by means of its own private key, the three parts will be sent to ASU together with signature. All the identification of certificates will be done by the ASU, when it receives the identification request of AP, it will first verify the signatures and certificates. When the identification succeeds, the certificate of STA will be validated. Finally, ASU will sign the identify results of STA and AP with its private key, then send the results and signature back to AP. AP uses the signature verification on received results, obtain identification results of STA, and decide whether to allow the access to STA according to the results. Meanwhile AP needs to transmit the ASU test results to STA, STA also verify the signature of ASU and get AP identification results, which helps to determine whether access to AP.

From the above description, we can see, WAI carried out a two-way authentication on STA and AP, so that it has a strong resilience against the "false" AP attack. The two sides will conduct a key agreement after certificates of STA and AP are the successfully identified. First of all, key algorithm negotiation will be
carried out between the two sides. Subsequently, STA and AP will each generate a random number, and transfer to each other after encrypted with their private key. Finally the two ends of communication will use each other’s public key to restore the random numbers generated by the other party, then make the results of the two random number mod 2 as the session key. With this key, we can encrypt communication data with prior exchanging algorithm. As the session key is not in the channel for transmission, and therefore enhance its security. To further improve the confidentiality of communication, WAPI also stipulates, after some time of communication or a certain amount of data exchange, STA and AP can re-negotiations the session key. Symmetric encryption algorithm is used by WPI on the encryption and decryption operations of MAC layer MSDU.

WAPI is designed in completely closed environment, so its main problem is not transparent enough. After the formal announcement of WAPI, domestic scholars have done some research on it; in general, there are still some deficiencies in WAPI design and implementation.

3.2. Security Analysis of Some Key Technologies

3.2.1. Security Analysis of TKIP

In the IEEE 802.11i specification, TKIP (Temporal Key Integrity Protocol) handles the encryption part of wireless security issues.

The length of TKIP key is 128 bits and packets using different encryption keys. Some different factors will be mixed together to produce the Key, including basic keys (i.e. the so-called transient key pairs of TKIP), MAC address of transmitting station and serial number of the packet. Hybrid operation will minimize the requirements in the design of wireless stations and access points, but still has sufficient password strength, so that it can not be easily deciphered.

As same as WEP, TKIP’s encryption is based on RC4, just different in the implementations. Although the WEP vulnerabilities has been settled, but TKIP can still be attacked through the shortcomings of RC4.

3.2.2. Security Analysis of EAP

Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication which can support multiple authentication methods. EAP didn’t specify authentication method during the link establishment period, but defer the process to certification stage.
So certification side can get more information in order to decide which authentication method to use. This mechanism also allows the parties of PPP authentication passing through the received certification packet to the authentication server at the rear, so that authentication server from the rear can realize a variety of authentication methods. WPA and WPA2 both can support to provide stronger authentication with EAP. The advantages of EAP can support multiple authentication mechanisms without having to specify in the pre-consultation process of LCP stage. Currently, EAP security issues are:

1. Identity Protection: Identity exchange is optional in the EAP, so it may be completely ignored.

2. Man in Middle Attack: When EAP run in other protocol, if the other side authentication is neglected, it will lead to a middleman attack.

3. Modify the packet: As EAP is to ensure the data packet’s source authentication, integrity and anti-replay, but this protection is not in the EAP layer, so an adversary can successfully insert or replay EAP packets by guessing identifier.

4. Dictionary attacks: Password-based authentication method (such as EAP-MD5, MS-CHAPv1) cannot resist a dictionary attack, so it needs to adopt some against-dictionary attacks.

5. Links to the untrustworthy network: EAP support one-way authentication (such as EAP-MD5), as the user don’t authenticate the authentication device, resulting in the user easy to be deceived by fake authentication device.

3.2.3. Security Analysis of LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a proprietary, previous variant before IEEE 802.1x port access protocol standards approved. 802.1x is a framework for a wireless authentication server approves the user to enter access point approved in the distributed network (i.e. access point to connect the wired network) before the wireless user authentication prior to the certificate. 802.1x works with many different certificates used together, such as passwords, tokens and certificates. This is done by the request and response to 802.1x carrying any type of EAP (Extensible Authentication Protocol) to complete. LEAP is one of these types of EAP, is designed to provide password identification.
LEAP is vulnerable for Dictionary Attack. First, the user name is not sent under encryption, everyone can get it. Second, the hash value generated by using words in the dictionary compared with the hash value generated by clients will be able to crack (or guess) the password. Some sharing software tools can automatically crack the hash value. These software tools include Anwrap, Asleap and THC-LEAP cracker. Using very long, random password will help prevent Dictionary Attack. However, this way round the leak is not practical, since many WLAN and existing user names (such as the Windows domain name) and password use LEAP together.

There are many other EAP types which can be used with 802.1x together. For example, EAP-TLS supports mutual authentication based on digital certificates. PEAP (protected EAP) support TLS encrypted channels in the MS-CHAPv2 password authentication, to prevent peeping and dictionary attacks. In fact, there are more than 40 kinds of definitions of EAP type. Some LEAP is weak (such as EAP-MD5), some is more powerful (such as EAP-TLS and PEAP). Of course, there are some types of EAP is more difficult to use than LEAP. For example, to use EAP-TLS, your client must have a certificate.

3.2.4 Security Analysis of PAP

PAP (Password Authentication Protocol) is a simple plain-text authentication. NAS (Network Access Server) requires the user to provide user name and password, and PAP returns information to user with plain-text. This kind of authentication’s security is poor, the third parties can easily get user name and password transmitted through eavesdropping, and use these information to connect with NAS and get all the resources available from NAS. Therefore, once the user password is stolen by a third party, PAP can’t provide guarantee measures to avoid attacks by third-party. Using PAP protocol, the whole authentication process is a two shook hands process, sending the password in clear text. PAP’s certification process is as follows:

(1) The verifier sends the user name and password to verify the validity, which is that the client requests to authenticate by the server-side;

(2) The server network checks whether the user exists and the password is correct according to its configuration information, and then returns a different response (Acknowledge or Not Acknowledge);

(3) If correct, the client will send the ACK (response
confirmation) messages, informing the other side that it has been allowed to progress to the next stage of consultation; otherwise, it will send NCK (non-confirmation) packet to inform the other side that confirmation has failed. But at this time it does not close the link directly, the client is allowed to continue to try new password. Only when the authentication fails for a certain number (the default is 4), the link will be closed, to prevent unnecessary LCP re-negotiation process caused by wrong transmission and network interference.

PAP authentication protocol is not in good condition and basically do not provide any security. Its feather is transmitting user name and password in a civilized manner by the network. If intercepted during transmission, it may cause a great threat to network security. So it is not a strong and effective authentication method. And the password sent in text format can’t provide any protection to against for eavesdropping, replay or repeat attempt and fault attacks, so it is only fit for this network environment which requires a relatively lower security. Compared with PAP, CHAP can provide a degree of security protection to password. Its authentication process is as follows:

(1) When the client requests a connection with the authentication server, it don’t input password directly by the client as PAP, instead, the server sends a randomly generated message with its host name to the client as an authenticate request;

(2) After the client receives the server’s authenticate request (Challenge), it checks the corresponding user account and password based on the server’s host name in that message and its own user table. If there is some account in the user table which is same to the host name, it use the random message and the user’s password received to generate response (Response) in Md5 algorithm, then its response and host name will be sent to the authentication;

(3) After receiving this response, the server checks its own reservation system password words in its user table by using the other’s user name, then generates results by using its own password words and random message in MD5 algorithm and compares with the proven party answers. If Successful, the authentication server will send an ACK packet (Success) and otherwise, it will send a NAK message (Failure).

The characteristic of CHAP authentication is only transmitting user name, not including user password on the network, so its security is higher than PAP. CHAP authentication method prevents replay attacks by using a different inquiring message and each
message is impossible to predict the unique values. Uninterrupted inquiry can be limited in a period of time among an attack, and the router local can control the frequency and time. However, the security of CHAP is still weak, with the attack technology’s constantly updating and improving, CHAP is attacked more and more, such as off-line dictionary attack, online dictionary attack, password leakage attack etc, so it is necessary to design more security password-based authentication protocol.

3.2.5. Security Analysis of PEAP

Protected Extensible Authentication Protocol PEAP (Protected EAP) uses Transport Layer Security (TLS) to create encrypted channel between client (such as wireless terminals) and the authentication device (such as Internet Authentication Service (IAS) or Remote Authentication Dial in User Service (RADIUS) server). PEAP is not specified authentication method, but provide additional security to other EAP authentication protocols, such as EAP-MSCHAPv2 protocol, which can be achieved by TLS encryption channel provided by PEAP. PEAP can be used for wireless client computer authentication in 802.11, but is not fit for virtual private network (VPN) remote access client or other clients. To enhance the security of EAP protocol and network, PEAP provides security protection as follows:

(1) The protection between the client and server in EAP method negotiation through the TLS channel. This helps to prevent an attacker inserting data packets between the client and the network access server (NAS), in case of the attacking to the less secure EAP method. Encrypted TLS channel also helps to prevent attacking against the refusal of IAS server;

(2) Supporting message and message fragmentation, allowing the use of EAP which does not provide this feature type;

(3) IAS or RADIUS server authentication. The server has to authenticate the client, so mutual situation exists;

(4) When the EAP client authenticate the certificate provided by the IAS server, the protection of deployment of unauthorized wireless access points (WAP). In addition, the TLS keys created by PEAP authentication server and the client are not shared with the access point. Therefore, the access point can’t decrypt messages protected by PEAP;

(5) PEAP’s fast reconnect, reduces time delay between the client authentication’s requests and IAS or RADIUS server’s response,
and allows wireless clients to move between access points without repeating authentication requests, which reduces resource requirements of the client and the server.

PEAP’s fast reconnect allows wireless clients to move between wireless access points in the same network without having to re-authenticate when associate with the new point each time. We configure the wireless access point as RADIUS client of RADIUS sever. If the wireless client roams between the access points which were configured for the same RADIUS server, the client don’t have the need to each authenticate for new client association. When the client moved to a different RADIUS client configured by different RADIUS server, though having to re-verify the identity of the client, but the efficiency of the treatment of this process is much higher. Because of the new server authentication requests forwarded to the original server, PEAP’s fast reconnect reduces the response time between the client and authentication server. As the PEAP client and authentication server both use the previously cached TLS connection properties, the authentication server can quickly determine whether the client connection is re-connected. If the original PEAP authentication device is not available, it must advance complete authentication between the client and the new authentication server.


According to Wireless broadband networks’ characteristics, technical characteristics and developing trends, and based on the study of multiple access subnets’ security standards and analysis. A security architecture is designed which has each layer’s security mechanism. This secure architecture can achieve safe goals such as reliability, controllability and availability.

4.1. Framework model

Wireless communication networks bring a great convenience to us; meanwhile, they face a series of new security issues, such as security between network entities, seamless connection among security protocols, and new security requirements of new various services. It is necessary to consider several important security issues in the process of developing wireless networks, including constructing a flexible wireless broadband network security model avoiding attacks, key security technologies and methods.

As network applications become more complex than before, the security requirements, especially the ability against attacks, are much more enhanced; it is true that people gradually take much more attention on network deep defense strategies. The ideal state
is that if a security system or a defense mechanism fails, the remaining security system and defense mechanisms will be able to provide the same level of security protection. It is necessary to embed the security features into each node. That is the security services and abilities extended to the node applications. And also it needs to design network’s program and network layer security mechanisms on the whole.

Based on the study of security standards of many access subnets, such as wireless LAN, wireless metropolitan area network, wireless wide area network, we find that when building a perfect security standards framework for wireless broadband system, it needs to refer to Open Systems Interconnection (OSI) protocol system model. Firstly, this chapter summarized security mechanism of access, network and application layer; secondly, security mechanisms are classified according to the strength of attacker’s ability. Finally, based on the work mentioned above, a model of "network layered, security classified and trusted domain departed" is proposed, this chapter also presented wireless broadband network security architecture on the basic of the access layer security.

4.1.1. Security Classification

Security protocol standards can be classified into general level, the weak and strong cipher level according to the security of cipher cell. General level protocol standard is a standard that focus on function realizing, security is considered low level security or even not, such as WEP, PEAP. Weak cipher level standard is a standard that fully considers security when established standard, but made a compromise between interests and security for commercial reasons, such as WPA1, still use the RC4 stream cipher system. Weak cipher level standard is also a standard that there are some weakness in its cipher security, or a standard that become insecurity because of enhanced attack methods. Although weak cipher security level standards are no longer safe, it is still consume enormous human and material resources to attack them; these standards are also useful in civilian application and some situation which doesn’t require high level security. Strong cipher level standard is a standard proved its safety by appropriate model, and also meet the new safety requirements, such as IKEv2; Strong cipher level standard is also a standard without proved its security under appropriate model, but until now there is not very effective attack to such standard, such as WPA2. If strong cipher level standard supports roaming and domain-crossing applications, it is necessary to consider the security when roaming and domain-crossing.
4.1.2. Security Domain

According to whether the authentication, key exchange protocol in security protocol standard supporting secure domain’s crossing or not, the security protocol standard can be divided into single trust domain, cross trust domain and heterogeneous network. Single trust domain is composed of wireless local area network (generally refers to the home network in mobile networks). There is a obvious boundary between single trust domain and Internet, user s can access the local information resources under the control of boundary secure measures. Cross trust domain refers to that networks belong to different manage organizations have different secure strategy and protective mechanism. It is likely to happen that a user under a secure domain communicates others in another domain in order to. This type connection can achieve resources sharing and information integrating. Heterogeneous network is a variety of coexisting heterogeneous network (communication network, WLAN, WiMAX, etc.). With roaming and domain-crossing within new generation broadband wireless mobile communication network become more common and complex and users’ high-level privacy protection mechanism given more attention, where the core is to solve the user’s security access and key exchange problem by using public cipher technology.

4.2. System Framework Content

According to present security protectionism, access security, key authentication technology state and developing trend, and based on the “sub-network layer, sub-safe level, sub-trust domain” standard classification model, a wireless broadband network security architecture is proposed as shown in Figure 1.
Based on the existing wireless local area network (mainly including WEP, IEEE802.11i, WPA security standards and WAPI), MAN (802.16 D3, 802.16E and Korea WiBro) and wide area networks (3GPP and 3GPP2 security technology system) standards, considering the national and international wireless broadband network security standards’ application status and coverage, aiming at our country wireless broadband network technology trend and network layout. Security architecture includes six safety technologies: heterogeneous network access security technology, password security technology, access control security technology, wireless intrusion and detection technology, mobile terminal security technology and mobile commerce security technology.

4.2.1. Heterogeneous Network Access Security Technology

Heterogeneous network has multi-trust domains, users, resources’ sharing servers and authentication service providers are belonging to different secure institutions. By studying identity-based USIM access authentication, smart card-based EAP authentication, fast re-authentication mechanisms, UE initial tunnel establishment and direct IP session access detecting mechanisms, we established a unified authentication model and security system structure for
heterogeneous network, which can shield otherness of different domains users, resources representation, security mechanisms, and can effectively harmonize domain-crossing information resource or access service in security. This system framework mainly include mobile network (TD-CDMA, WCDMA, CDMA2000) and local area network (WLAN) access security standards, and mobile network (TD-CDMA, WCDMA, CDMA2000) and wide area network (WIMAX) access security standards.

This standard not only will enable trusted domain-crossing (including roaming case) authentication and key agreement, and resolve the mutual operation of heterogeneous network (secure domain-crossing) and security establishment. This standard can achieve two main objectives, the first one is that when users roaming other service provider area, they can validate whether the provider is a legitimate one or not and, meanwhile the service provider also can validate whether the user is a legitimate one or not, but also this standard can produce session key in the process of domain-crossing authentication which can guarantee the data under a safe model. A more promoted domain-crossing authentication security model is proposed under standard model or random predictive model by excavating the content of computational problems and using international advanced security-provable method. We analysis the secure qualities of this model via using Oracle model and formalized tools, and we also analysis and test the performance of this new protocol. Key agreement protocol must meet several important security goals, such as fake attack due to key leaking, unknown session key sharing attack, and forward security and so on.

4.2.2. Password Security Technology

Current domain-crossing password authentication and key exchange protocol are designed largely based on symmetric key mechanism; they cannot prevent new type attacks (PCI, KCI). Now public key cipher mechanism is always be used to enhance protocol security, but it undoubtedly increases the quantity of online computation, the burden of network and the times protocol information transmission. So it is very valuable to design a certifiable secure domain-crossing password protocol for which has several good characteristic such as low-transition times, tradeoff security and efficiency, and broad application market. Protocol of provably secure cross-domain password with safety and efficiency, especially in the mobile environment, and this has a wide range of application environments. Meanwhile, the user to user password security technology research and design for different security domain are also valuable.
The way to describe the ability of attacker, simulate attacker and participator’s action and extend the current secure model to meet advanced secure attributes must be reasonable. So a more complete cross-domain password authentication and key exchange security model can be established.

Generally speaking, network server have public key in practice, nor do mobile terminals, so in the protocol designing, it is sensible to take full account of asymmetry between terminal and server, make optimization analysis of the protocol participants’ number of computation and interaction and minimize the amount of mobile terminal computing when designing effective, lightweight, domain-cross protocol.

The secure evidence of draft candidate provided by international organizations have a principal limit of the random oracle model or ideal code model, and to some extent rely on public key encryption system. So, in addition to basic nature of security mentioned above, the feasibility of efficiency, the security within standard model, getting rid of relying on public encryption and other factors affecting security and efficiency, are also considered when design password protocol. From the existing candidate password standard draft’s analysis, password secure technology should satisfy some basic secure features:

* Resist off-line dictionary attack
* Resist on-line dictionary attack
* Satisfy forward security
* Resist server destroy attack
* Resist Denning Sacco attack (gotten the assigned session key have little help to adversary)

4.2.3. Mobile Terminal Secure Technology

As fast development 3G networks, the number of people who use 3G terminal device will become larger and larger. More and more personal information will be stored in terminal equipment. The privacy and the importance of personal information are often higher than other information stored in individual hosts. Therefore, Mobile terminal particular secure requirements are higher.

Product and service providers embed security technology in the mobile device to ensure platform crossing computing and
communication security and interoperability. These security solutions are mostly operated in the operating system. However, these operating systems are very complex, which makes a big problem to get a stable security just relying on an operating system alone. Furthermore, implementing security in the operating system also significantly prolongs the process of developing and debugging. Therefore, it is necessary to standard intelligent terminal’s security function.

On the other hand, the current intelligent mobile communication equipments of 2G and 2.5G networks have following secure problems: lack abundant security defending software, low firewall usage rate, users’s security awareness of mobile communication device is less than personal host.

(1) Access security and Data security

Mobile internet terminal should have the authentication function; have the ability to access control various system resources and service applications. The terminal secure technology needs to consider identity authentication using password, smart card and entity authentication mechanism. For data security protection and access control, setting access control policy can ensure their safety; Hierarchical storage and isolation, data integrity detecting and other measures can ensure the security of data stored within the terminal.

(2) Terminal security protection mechanism

Terminal security measures are proposed to protect the safety of various types of hardware and software systems (operating system security), data security and content security, and avoid illegally juggling information, unauthorized access and the malicious access caused by viruses and malicious code. Technical specifications and relevant parameters are suggested by using tools such as firewall technology, intrusion detection techniques, and Trojan detection technology.

4.2.4. Access Control Technology

Access control is to permit or limit access ability and extension by some approaches, and thus Access control can limits visiting to secure protective resources, and prevent destructions caused by the illegal user’s malicious invasion or legal user’s careless operation. Because the changes and development of computation environment and the resource sharing patterns, access control face the brand-new challenges. Especially due to the existing authentication and authorization technology’s poor support to
heterogeneous environments, poor system scalability, thick granularity and bad dynamic access control, high cost, so it is impossible to meet requirements of large-scale resource sharing applications. Therefore, we should use some key technologies, such as domain crossing authentication, authorization management, and dynamic thin granularity access control, to implement the access control in the new type networks and applications.

(1) Access control model

Access control model which is suitable for domain-cross environment can support multi authorized attributes (including secure attributes of subject, object body, and operation the relationship of network elements). This model can support many kinds of access control strategy (RBAC-based access control, identity-based access control and so on), and can thick granularity and too complex problem of single model is solved. How to integrate the area concept into the access control model is explored (via attribute or other ways). Then, the subject and object security attributes modeling methods are researched, thin granularity can be achieved by defining attributes of thin granularity. This segment also investigate attribute-based access control model which can support multi type secure strategy, attribute layer model and giving a common and flexible attribute layer framework. Collision avoiding scheme which can support multi strategy is studied. The constraint mechanism of attribute-based access control model is researched (including duties separation and constraint tense, etc.).

(2) Multi-domain strategy integrated technology

In order to realize the resource sharing and protection between different trusted domains, we need to integrate each domain original access control strategy to obtain a unified overall access strategy. Strategy integration follows autonomy principle and security principle. Attribute-based access control can express the traditional access control strategy by using uniform attributes and authorization framework, therefore its integrated method is also applicable to integrate traditional strategy. We research on the attribute-based access control integrated framework, the accuracy of its integrated result can be ensured via semantic form. Strategy collision detection algorithm is also investigated, this algorithm can detect automatically circular inheritance and constraint destroy of integrated strategy attributes layers, and can automatically clear up collision in the process of strategy integrating. This segment also researches on efficient modular algorithm of integrated strategy; this algorithm tries its effort to avoid the global integration when there is a small change in strategy.
(3) User authorization attributes’ privacy protecting technology

When the user access to resources across trusted domain, the resources provider may cross other domain to index the user’s security attributes. Users usually do not hope their privacy information to be known by others in another trusted domain when accessing. So, the inter-agency access to resources often need to ensure the anonymity of their users, and must provide privacy protection of users attributes during cross-domain indexing. This project researches on protection strategy and realization mechanism to protect privacy of users’ authorization attributes, and, investigate the thin granularity users’ self control privacy protection mechanism which allow users to choose the disclosed attributes by themselves, and study how to negotiate the access attributes step by step in the process of access control to minimize the leakage of users privacy attitudes.

(4) Frame design with dynamic context support

The key to realize dynamic access control is that the context (environment) information in the process of strategy estimation when access request happens. Now, many access control strategies support context-based access condition information. When estimating strategies, appropriate context provider must provide context information to strategy engine. In this project we will research how to provide a dynamic context supporting frame, which can integrate the various service providers transfer interfaces, the corresponding service provider module, and one or more software or hardware-based context inductor. Common framework of context providers is investigated and the standard access interface and communication interface are defined, how to get reliable context information to ensure making accuracy strategy is also considered.

(6) Access control strategy algorithm and access strategy engine design

The performance of access control strategy algorithm can decide the performance and throughput of the strategy engine. We research on the search algorithm (that is, making a determining of the applicable strategy or rule algorithm according to strategy request) of strategy request. We also research on search algorithm of subject, object body and the environment attributes’ acquisition mode and the applicable attributes when decision-making. Efficient evaluation algorithm of advanced access control strategy, and updated algorithm of the evaluation intermediate results which stored in cache for improving algorithm performance is also
studied, performance evaluation mode of the access control decision engine is investigated at last.

4.2.5. Wireless Intrusion Detection Technology

There is a great deal of differences between wired and wireless network, it is impossible for wireless network to directly employ the intrusion detection system (IDS) which was designed for wired network. The reasons can be list in the following, firstly, traditional IDS largely depends on monitoring and analysis of the entire network real-time services, but wireless networks can only provide partial data information for intrusion detection, because we can but get the data which is restricted within the wireless communication range. IDS must employ these half-baked data information to achieve intrusion and detection. Secondly, the link of mobile network is slow, the bandwidth is limited, and the nodes rely on battery to supply power, these features make that it has very strict demands on communication and does not adopt the communication protocol designed for wired IDS. Thirdly, there is not an obvious boundary between normal and in normal operation due to high-speed mobile network topology changing. The nodes sending wrong messages may be the captured nodes or nodes temporarily losing synchronization due to fast moving. Generally, it is difficult for IDS to identify the real intrusion and the temporary system malfunction. Thereby, we think that the main point of wireless intrusion and detection standard research is technology investigation. A pertinent standard will be instituted based on the application level of network until the technology become very advanced.

At present, there are mainly two intrusion and detection systems reputed: distributed intrusion-detection system based on mobile agent, ad hoc network distributed intrusion-detection system. The former’s core is mobile agent module. Based on the different function of number limited mobile agents in ad hoc network, mobile agents can be distributed to different nodes, and execute different intrusion detection mission. An action implementing model can take appropriate measures according to the final test results. As the number of mobile agents are significantly reduced, this intrusion-detection system model has lower network overhead than other IDS. Ad hoc network intrusion detection system requires all the nodes in the network to participate to detect intrusion and make response. Each node is equipped with an IDS agent, the IDS agents using a statistical abnormity-based detection technology. When a node makes an exceptional report, the IDS agents in different regions co-operate to launch global intrusion detection and make response. In the security research of ad hoc and cellular integrated network, CAMA structure discussed intrusion detection.
If an intrusion node is detected, CAMA agent will broadcast security information to the entire network through base station. The mail function of intrusion detection is to solve routing security issues caused by CAMA nodes deliberately provide incorrect location information to the base station. When a node receive a routing table from base station, and finds that the next hop node does not exist, then it sends a wrong routing report to the base station. CAMA agent finds out the malicious node then kick it out from network.

With the rising risk coefficient of network security, in addition to improving the conventional and traditional techniques (pattern recognition and integrity detection), network intrusion detection system should take much attention to investigate statistical and analyzing technologies, we suggest the specific requirements and specifications of the detection range, the percentage of system resource accounting and warning accuracy probability by combining with new methods such as distributed intrusion detection, application layer intrusion detection and intelligent intrusion detection. Future technology trends can be embodied in the following aspects:

(1) Coexistence of detection and firewall technology

Basically speaking, detection techniques represented by IDS are very different from access control technology represented by firewall. Firewall is a gateway format; it requires high performance and high reliability. So the firewall pays attention to requirements of throughput, delay, and HA. The main features of the firewall are passing (transmission) and off (blocking) functions, so requirements of transmission rate are very high. The features of IDS are detecting and discovering, its goal is to decrease the probability of lost and miss record. In this sense, detection and firewall technology will concern each own characteristics in a long period of time. Their performance and reliability are enhanced dependently; they cannot replace each other or simply integrate together.

(2) Cooperation of detection and access control is an inevitable trend

Although there are some differences between detection and access control technology, it is an urgent requirement and inevitable trend that the two technologies work together and integrate their application. The integration of security products, collaboration, and centralized management is a trend of network security. Large enterprises need integrative security solution schemes and thin granularity security control methods. In one hand, the less large
enterprises want to get practical security guarantee, on the other hand, they do not want to invest much money to ensure information security. From the early active response intrusion detection system to the linkage of intrusion detection systems and firewalls, and to the IPS and IMS, they form a continuous improving process of solving security needs.

(3) Integration of multiple technologies is the future trend

The point of view, "centralized detection, distributed control" is very important to how to consider the trend of detection and access control technology. IDS which is not entirely satisfied can become accuracy by manual analysis. Similarly, a more accuracy result will be achieved though centralized detecting and associated analysis with other detecting technologies after large-scale IDS deployment. Thus, overall events detection will replace partial events detection. Overall response and control can be implemented according to the overall detecting results.

In conclusion, as a proactive security guard technology, the intrusion detection system provides real-time protection of internal attacks, external attacks and miss operations, and make a interception and response to the intrusion before endanger the network system. With the increasing secure demands of network communication technology, in order to provide reliable services for e-commerce and other network applications, intrusion detection systems can provide secure services from the point view of tridimensional depth and multi-level defense of network security. People will pay much more attention to intrusion detection systems in future.

4.2.6. Mobile E-commerce Secure Technology

The defending ability of mobile e-commerce can be enhanced by investigating technology and increasing the standardization of secure technology in the mobile e-commerce application process. Mobile secure technology protects important information of merchants and customers in the mobile commerce, and maintains the credibility and property of the business system. It is obvious that mobile e-commerce can be used and extended no other than taking appropriate secure technology. Though many secure technologies should be investigated, the crucial technologies of mobile e-commerce must stress much more efforts to get evolution and form a standard. The crucial technologies are expressed as follows:

(1) End to end secure strategies. As for mobile e-commerce service, end to end security means that each feeble part should be protected; data transmission from source node to destination is absolutely safe, including each stage of the transmission process.
That is looking to find every weak point and to take appropriate secure and privacy measures to ensure that the transmission process each channel is safe. Mobile e-commences have brought a lot of equipment, they run different operating systems and employ different standards, so safety has become more complex;

(2) Employ WPKI technology. End to end security of data transmission, users’ secure authentication and reliable transaction, can be achieved via deploying wireless public key infrastructure (WPKI) technology. WPKI uses public key cryptography and opening standard technology to build credible security architecture which can facilitate transactions and secure communications authentication in public wireless network. Reliable PKI can not only authenticate users, protect the integrity of data transmission and confidentiality, but also can help enterprises to implement non-replication ability, so as to prevent parties deny their transaction;

(3) Identity authentication. Strengthen the bargainer identity recognition management. In the mobile commerce transaction process, the accuracy of users’ access and authorization is guaranteed by strengthening the management of users’ identity authentication. The behalf of two parties in transaction is not damaged via the real identity authentication;

(4) Mobile payment. As the mobile payments are often happen in an open environment of mobile Internet, the parties of the transactions may not trust each other. In many cases, there are many dissensions in transactions, so fairness of transaction plays an important role in mobile payment. The so-called fairness of transaction refer to two parties achieve each dealing goals or not when the transaction is over. Each party is equal to others when implement mobile payment protocol.

In addition, mobile payment must consider protecting the anonymity of user’s privacy. Businessman, listener-in and banks like anonymity, the current system achieved that businessman and listener-in do not know the identity of users, but banks know the users’ real identity. Mobile payment does not completely realize incapable tracking of users and mobile payment, and also the unable payment linking. In addition, because of anonymous mobile payment characteristic, honest users are easily deceived by dishonest users, so it is necessary to repeal the anonymity of dishonest users.

5. IANA Considerations
6. Security Considerations

The content of the Category header-field is not secure, private or integrity-guaranteed, and due caution should be exercised when using it.

7. References

7.1. Normative References


Author’s Address

China National Digital Switching System Engineering&Technological R&D Center
No. 780, BOX 1001
Zhengzhou, Henan, 450002 P.R.China
Phone: +86-0371-81632917

EMail: rxmhkz@126.com