uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Jeong Ja Kong
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.Sc. (Systems Science)
GRADE / DEGREE

Systems Science
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Security Systems for Passive IP Devices on Sip-Based Networks
TITRE DE LA THÈSE / TITLE OF THESIS

T. Yeap
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

V. Groza

A. Nayak

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

SECURITY SYSTEM FOR PASSIVE IP DEVICES ON SIP-BASED NETWORKS

Jeong Ja Kong

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
for the MSc degree in the Master's Program

Systems Science
Faculty of Graduate and Postdoctoral Studies
University of Ottawa

Your file Votre référence
ISBN: 978-0-494-59464-3
Our file Notre référence
ISBN: 978-0-494-59464-3

Abstract

Session Initiation Protocol (SIP), an easy and simple Internet application layer protocol used to establish a session, and passive Internet Protocol (IP) devices like SIP-based surveillance cameras, form a perspective combination that is on demand in the network market. The only necessity of the predefined network is to acquire a secure mechanism due to the private information that the devices transmit on the Internet network. This thesis proposes an architecture for securing information that passive IP devices deliver into public IP networks. The architecture provides a security mechanism for authentication, authorization, and audit (AAA). The mechanism combines the security features of the authentication server with SIP architecture to provide AAA service to registered users requesting access to passive IP devices. Also, the Authentication-Authorization Database (AADB) that allows device certificate management is introduced. The dynamic password and dynamic session key utilized by the Public Key Infrastructure (PKI) scheme are also introduced to enhance the security features of devices by authenticating and administering user accesses and device accesses. The AAA with the authentication database and dynamic authentication mechanism ensures a secure IP network based on SIP protocol.

Acknowledgements

Thank you, Dr. Tet Yeap, for giving me great advice and showing me a good model of energetic life. You have made a deep impression on me.

Thank you, Natalie, for teaching me English and sharing your time with me.

Thank you, Jeesu, Byoungchan, Byougwhee, and Meyng-hoon, my precious family. The forbearance of all of you was another prize that was given to me.

Thank you, God. You have given me everything I needed.

Contents

List of Tables

List of Figures

Abbreviations

AA Server	Authentication-Authorization Server
AAA Server	Authentication-Authorization-Audit Server
AADB	Authentication-Authorization Database
CA	Certificate Authority
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server

Chapter 1

Introduction

1.1 IP Network, SIP and IP Devices

The Internet has become the most powerful tool for the transportation of information and communication from and to people and network devices. Network devices on the Internet transfer data and information, including conversations and images, by means of standardized protocols. Protocols are the languages that have been used on the Internet network, and communication networks integrate many protocols and some application software, which is often referred to as a protocol stack, to provide specialized services.

According to the Open System Interconnection (OSI) reference model, which is a famous example of the network model and is well illustrated practically, the seven layers perform their specific tasks in the network communication. Transmission Control Protocol (TCP) is a connection-oriented protocol that establishes connections before sending and receiving messages and one of the fourth-layer protocols that work at the transport layer, which provides reliable data communication schemes by end-to-end error handling and transfer flow control and by utilizing acknowledgments and sequence numbers to assure that the message arrived safely at its destination [1]. Another well-known transport layer protocol

is User Datagram Protocol (UDP), which is a connectionless transport protocol and transaction oriented. Connectionless transport service is used to send non-critical or short messages, because reliable message delivery is not guaranteed. The advantage of this connectionless protocol is a minimum set of protocol mechanisms and faster performance [1]. Internet Protocol (IP) is a network layer protocol that routes data-grams from one network device to another across an inter-network by addressing and fragmentation.

One of the most widely used protocols in the public Internet is the TCP/IP protocol suite. The protocol stack consists of a network-layer protocol like TCP or UDP and a transport layer protocol IP. TCP/IP protocols enable the routing by using IP addresses to identify the destination and the source of the data. The HTTP (Hyper Text Transfer Protocol) [2] which works over a TCP/IP connection is a request/response protocol, and the protocol provides several optional challenge-response authentication mechanisms that can be used by a server to challenge a client request and by a client to provide authentication information. Multipurpose Internet Mail Extensions (MIME) is an Internet standard that defines the format of messages to allow for textual message bodies in character sets, and Secure/Multipurpose Internet Mail Extensions (S/MIME) [3] supports authentication, the message integrity and the non-repudiation of origin, and privacy and data security by adding cryptographic signature and encryption service to MIME data such as HTTP.

Session Initiation Protocol (SIP) ([4], [5]) is a simple application-layer control protocol that can establish, modify, and terminate sessions. SIP is a signaling protocol that manages communication sessions between two processes, which are session creation and termination, and is one of the leading signaling protocols for Voice-over IP, along with H.323 ([6], [7]). In addition, SIP has been chosen for multimedia applications in 3G mobile networks by the 3rd-Generation Partnership Project (3GPP), and also it can be a part of an IP multimedia

subsystem (IMS) [8] to provide access to multimedia and voice applications across wireless and wire-line terminals. Also, SIP supports IP phone services like peer-to-peer IP telephony [9] and multimedia conference. Thanks to its simplicity and ease of access and use, lots of SIP-based applications like Skype [10] have already been introduced to the public.

1.2 Thesis Motivation

SIP-based surveillance cameras are about to enter into the IP devices market to contribute in the area of multimedia distribution [11]. The demand of such IP network-based surveillance devices is increasing according to the development of easier telephony signaling protocols, while the management and installation cost of the coaxial cable system, which is a dedicated signal transmission line, takes a superior position when it is compared to the cost of an IP-based LAN network. In addition, digital information can be directly transported to the destination point on the network without having to apply any signal transformation, making the architecture ideal for network-based applications. Moreover, switching to an IP network from a coaxial transmission system brings more freedom in locating the management part on the network. The coaxial cable system has more limitations when it is employed with passive devices on the network. First of all, the transport distance is limited in relation to the cost of maintenance devices and management system configuration. The second problem is its transport direction and related costs. For the bidirectional transport network, the cost doubles. Contrarily, the IP network is already being used by the public, and its transporting distance is increased with the support by the network devices like repeaters, routers, and other intermediary servers.

However, the application of passive IP devices in the public Internet poses many security problems, which include feasible attacks. Therefore, we need to address that before it can be widely accepted by users. In this thesis, novel security architecture is discussed and proposed to address and solve some of the security concerns.

1.3 Thesis Objectives

The main objective of this thesis is to introduce a secure SIP based network composed of IP devices. When the deployment of surveillance devices into the IP network is considered, priority is placed on the protection of message privacy and secure management because of private characteristics of the information that the IP devices would deliver to the public network and because of passive characteristics that would easily allow anyone who knows the SIP address and password of the device to tamper with the device and the private information on the IP network.

As expected, when any secure mechanism is considered and established in the combination with the simplicity of network communication achievement at the same time, IP devices are safely and easily located in the public network, especially with simple session initiation protocol SIP. When the secure architecture for the SIP-based IP network is discussed in this thesis, some features of the proposed architecture are demonstrated by comparing them with other authentication mechanisms.

1.4 Contributions

In this thesis, the concepts of access authentication and device authentication are introduced, and security consideration about passive SIP devices is discussed. In addition, the necessity of device and network management by using access authentication, device authentication and device certificate, which are essential to enhancing the network security for passive network devices, are emphasized and manifested.

Secondly, authentication mechanisms and authority management in the suggested network frame promote the IP network security, especially securing the SIP-based IP network in which passive devices are the network entities and deliver non-public information, in terms of user authentication and device authentication, as a secure mechanism. The architecture, which employs dynamic password scheme and dynamic session key scheme based on PKI infrastructure, upgrades network security.

In addition, the suggested administration method of the SIP network for passive IP devices gives an idea for similarly designed network management. The proposed administration utilizes the AA database and device certificates to manage the network system, control user access flow to passive devices, and suggest the predesigned authorization policy for users and device authority. The AA server can execute more administrative functions like audit by working together with the AADB.

1.5 Thesis Organization

Most security concerns about the network and the characteristics of SIP are discussed in the proceeding part, and security considerations about passive IP devices are discussed in detail

in C*hapter 2*. *Chapter 3* deals with access authentication, device authorization and the audit of passive IP devices operating in a SIP-based IP network, and another authentication method for SIP is introduced, and how dynamic session key works is discussed in the SIP network with passive devices in *Chapter 4*. In *Chapter 5,* the comparison between the methods of *Chapter 3* and *Chapter 4* is given. Then the conclusions, *Chapter 6*, follow.

Chapter 2

Security of the SIP-Based IP Network

2.1 Network Security Concerns

In any network, secure networking is a matter of increasing concern, so most network administrators try to build secure networks. As a matter of fact, the meaning of the word "security" differs from network to network, and the way of building a secure network and the level of the security also varies according to their implementation in the information technology area. For example, in the book "The 3G IP Multimedia Subsystem" [8], the author says network security is comprised of mechanisms that provide integrity, which provides message integrity and the proof of the data's origin; confidentiality, whose mechanisms keep unauthorized parties from getting access to the contents of messages; and availability, which is an ability to protect authorized users from the attacks like Denial of Service (DoS) that is keeping authorized users from accessing a particular service. In another book [12], the authors say that the communication security requirements are the integrity, authentication, and confidentiality of the network. Here, integrity means to confirm the message has not been altered during transmission, and authentication means to ascertain that

the sender is who s/he claims to be. Confidentiality means that the information should be readable only by the intended recipient. Finally, the network security should be newly defined according to the various network characteristics like, for instance, type of business, type of data, and network management philosophy.

2.1.1 Cryptography

To ensure the authenticity and secrecy of the message being transferred between end entities, various kinds of cryptographic technology are implemented. The main categories of cryptography are symmetric, like Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and asymmetric key algorithms like Diffie-Hellman and RSA, which is also used for digital signature algorithms [13]. The symmetric key algorithm uses the same key for encryption and for decryption, but the asymmetric key algorithm, which is sometimes called the public key algorithm, uses a different key for encryption and for decryption. In a short comparison, symmetric key algorithms are known to be generally much less computationally intensive than asymmetric key algorithms. From a key management view point, one disadvantage of symmetric key algorithms is the requirement of a shared secret key, and moreover, the shared key should be changed regularly and kept secure during distribution and in service for the purpose of protection from potential discovery by a cryptographic adversary.

2.1.2 Authentication

Generally, to acquire some level of security, all network entities should reliably learn the identity of the originator of a message or request between each other, whether the network is peer-to-peer network or client/server network. In a client/server network, the server should

know the identity of the upcoming network client, and at the same time, the client should make sure that its contacting server is not an impersonating one. In the same way, in a peer-to-peer network, the end network entities should know each other in the communication period. Therefore, all the network entity might prove its identity when it sends messages or requests to the other side entity of the network. The process of identification is defined as the authentication in the network, and the goal of authentication is to reliably learn the name of the originator of a message or request. Authorization is another part of secure network management and is the process of allowing network resources to be used by network entities that have been granted the authority to use them. When an agent is going to access the predefined network, or when a device is going to access into the network which has to be protected from an unidentified third party, the authentication processes for each process are needed. As discussed in the IETF RFC 2904, there are a large number of authentication applications in accordance with the network entities, trust relationships, designed network service types, and the authorization policy of each organization.

According to the origin trusted party which gives insurance of the entity's identity, authentication method is named as self-authentication or third-party authentication. In general, third-party authentication gives us a more trustable tool than self-authentication does in an authentication mechanism. If the two joining parties trust the third party, then the identification of a coming party by the third party can be accepted by the network. The third-party authentication involves the authorized or certified authentication agencies for the purpose of managing the network and certificate certified by the authorized agency. On the other hand, IETF RFC 1508 suggests that an encryption mechanism is used to authenticate each other side in a strong and mutual way in a distributed environment. According to the document, there are two steps in the authentication process, which are the identification step

and the verification step. The identification step is to present an identifier to the security system, and the verification step is to present or generate authentication information that corroborates the binding between the entity and the identifier. In the process of identification, identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control services and also authentication is related to data integrity.

One of Authentication servers, which is for Remote Authentication Dial-In User Service (RADIUS) authenticates users by authenticating user identification information delivered from Network Access Server (NAS), and can be another proxy client server for other authentication servers [14]. RADIUS is a protocol which carries authentication, authorization and accounting information between NAS and RADIUS server, and a prepaid mechanism for VoIP and messaging service is proposed by combining RADIUS server and Back-to-Back User Agent (B2BUA) to authenticate prepaid users for the service [15].

Some authentication mechanisms provide authentication in the link establishment phase. IETF RFC 1334 defines two authentication protocols, Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP), for PPP (Point-to-Point Protocol). In the PAP authentication method, passwords are sent over the circuit clearly, but CHAP is stronger than PAP and is used to periodically verify the identity of the peer using a three-way handshake; after the link establishment phase is complete, the authenticator sends a unique and unpredictable "challenge" message to the end entity. The end entity responds with a value calculated using a "one-way hash" function. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged.

IETF RFC 2617 [16] suggests two access authentication schemes in HTTP authentication, basic authentication and digest access authentication. This basic scheme is not considered secure user authentication if it is not combined with other external secure mechanisms such as SSL, for the reason that the user name and password can be seen as clear-text over the network. Like basic authentication, digest access authentication verifies that both parties to a communication know a shared secret; for example, a password. Unlike basic authentication, this verification can be done without sending the password in the clear, which is basic authentication's biggest weakness. The basic authentication scheme is based on the model that the client must authenticate itself with a user ID and a password for each realm. Like basic access authentication, the digest scheme is based on a simple challenge-response paradigm. The digest scheme challenges by using a nonce value. A valid response contains a checksum of the user name, the password, the given nonce value, the HTTP method, and the requested URI.

As mentioned earlier, S/MIME provides the cryptographic security services such as authentication, message integrity, and non-repudiation of origin using digital signatures, and privacy and data security using encryption. S/MIME provides a method to send and receive secure MIME messages, and certificates are an integral part of S/MIME agent processing. Before using a public key to provide security services, the S/MIME agent must certify that the public key is valid. S/MIME agents must use a Public-Key Infrastructure (X.509) (PKIX) Certificate to validate public keys; as described in IETF RFC 3280 [17].

Public key cryptography is asymmetric cryptography, in which a sender encrypts the plaintext using a public key, and the message receiver decrypts the cipher text by using a private key [12]. X.509 is an ITU Telecommunication Standardization Sector (ITU-T) standard for PKI and a public-key technical mechanism for communications security. IETF

RFC 3280 supports an X.509-based PKI, the X.509 v3 certificate format, and the X.509 v2 Certificate Revocation List (CRL) format for use on the Internet and describes an algorithm for the certificate path validation, an algorithm for determining the status of a certificate using CRLs, and the information describing the use of delta CRLs. It allows applications like WWW, electronic mail, user authentication, and IPsec [18] algorithm identifiers, and ASN.1 encoding formats for digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKI) is specified in the document RFC 3279. The document also supports one-way hash functions like MD2, MD5, and SHA-1 and signature algorithms like RSA (named after its inventors, Rivest, Shamir, and Adleman), Digital Signature Algorithm (DSA), and Elliptic Curve Digital (ECD), which may be used to hash data and to sign certificates and CRLs. In addtion the document identifies object identifiers (OIDs) for public keys contained in a certificate. Certificates include the public key of the named subject. "The data, which is the one-way hash function output value, to be signed is formatted for the signature algorithm to be used. Then, a private key operation is performed to generate the signature value. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate or Certificate List in the signature field." [19]

Digital signature mechanisms are often used for entity authentication and data origin authentication. In X.509 PKI, two protocols such as operational protocol and management protocols are needed to deliver certificates and CRLs or status information to certificate-using client systems and to support on-line interactions between a PKI user and management entities, which can be registration, initialization, certification, key-pair recovery, key-pair update, revocation request, and cross-certification. The Grid Security Infrastructure's [20] single sign-on and delegation capabilities, built on X.509 proxy certificates [21], also are being employed to provide authentication services to these applications. Otherwise, there are

many applications that construct a certification path and then validate the certification path [21].

Protocol for Carrying Authentication and Network Access (PANA) ([22], [23]) PANA is another protocol that may provide a way of carrying authentication information securely. With PANA, residing or separated authentication server may be implemented to provide secure authentication mechanism by using other authentication protocol like RADIUS according to PANA functional model [23].

With regard to the authentication mechanism, many papers have been produced in the network security point of view, which is based on the authentication scheme and authentication mechanism. For example, one paper [24] discusses how to express agent beliefs involved in authentication protocols by utilizing a belief logic called BAN [25] and by evaluating the belief logic after a series of observation of clients as a consequence of communication. Another research paper [26] deals with secure methods of authentication based on password authentication by utilizing the Single Sign On (SSO) feature on password-based authentication protocols like Kerberos [27], which is partly based on Needham and Schroeder's trusted third-party authentication protocol and on password-based authentication protocol.

2.1.3 Directory Service for Authentication

When the PKI is implemented, methods of finding the certificate of the CRL issuer are currently available; for instance, through an accessible directory location. For example, end entities may publish their own certificate in the repository using FTP or HTTP, and the FTP and the HTTP need to obtain certificates and CRLs from PKI repositories.

Directory lookup requires the existence of and access to a directory that has been populated with all of the necessary certificates. The X.509 directory service is one of the directory services for authentication, and the Lightweight Directory Access Protocol (LDAP is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.

2.2 Secure Mechanism

Lots of research has been focused on the security mechanism in the inter-network area, and those topics cover secure operation and management protocols, factors of authentication, level of authorization, network access control, etc., which have relationships with integrity, authentication, and privacy. We need to look into the mechanisms that provide message integrity, authentication and privacy.

Message integrity ensures that if the third party modifies the message being transferred between end-entities, the receiver is able to detect the modification as well as that the messages are transported to the intended right destination without losing any messages. For integrity, usually IP headers keep the host location information and presence so that IP headers are readable by the network router and the header cannot be encrypted for the reason of routing the message to its designated destination.

When two hosts, which include intermediary network entities like proxy servers, exchange the data, they can protect the transmitted information from being clearly readable by encrypting the data packets. Symmetric encryption algorithms like DES or public key encryption algorithms like Diffie-Hellman and RSA work for message confidentiality, besides integrity checking. In addition to the encryption, the digital signature adds more

protection to the messages. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message (or a hash of the message or both), and one for verification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes such as SSL/TLS [28]. The process of selecting, distributing, and storing keys is known as key management; it is difficult to achieve reliably and securely.

End-to-end encryption can be the strongest protection from outside attack, but in the current IP network environment, it is not feasible to use end-to-end encryption for the reason that there are lots of intermediary servers and proxies that are helping networking on the IP network. For example, application-level gateways or proxies have been developed to enforce the security at the level of specific services. Circuit-level gateways restrict the TCP connections that are allowed across them, so the end-to-end connections are not allowed and must be broken into pieces to get through the firewall system [29]. Usually, the hop-by-hop network devices must be deployed on the IP network to provide the specified network application service to users broadly.

Therefore, we need to find out and to classify the feasible network attacks to figure out how to protect information and network services from being used in unexpected ways. There are attacks that are well-known to the public as serious attacks for network systems regarding network integrity and confidentiality. These attacks are eavesdropping, registration hijacking, impersonating a server, message modification, tearing-down sessions, denial of service (DoS) and amplification, and message re-play. They affect the network confidentiality (or privacy), integrity, and availability with regard to secure mechanisms in the network.

Table 2-1 shows the relationship between attacks and their influences on network security factors.

Table 2-1 Relationship Between Network Attacks and Security Factors

Security Items / Attacks	Integrity	Availability	Confidentiality
Eavesdropping			✓
Registration Hijacking		✓	
Impersonating a Server	✓		✓
Message Modification	✓		
Tearing Down Session		✓	
DoS and Amplification		✓	
Replay			✓

2.3 SIP: Session Initiation Protocol

SIP is a signaling protocol that manages the communication sessions between two processes, which are session creation and termination, and it is one of the leading signaling protocols for Voice-over IP, along with H.323 [30]. It is designed to operate above the transport layer of the underlying network for real-time point-to-point audio communication between two terminals on a packet-based network that does not provide a guaranteed QoS by itself. The main signaling functions of SIP are a destination entity location, contacting the destination entity to determine its communication willingness, negotiation of media parameters for establishing sessions, and modification of existing media sessions.

SIP can be used as an independent component of the featured network communication service in concert with other IETF protocols "such as the Real-time Transport Protocol (RTP) for transporting real-time data and providing QoS feedback, the Real-Time streaming protocol (RTSP) for controlling delivery of streaming media, the Media Gateway Control Protocol (MEGACO) for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP)" [4], which describes the media content of the session, e.g. what IP address and port number to use, media transport protocol, and the codec being used, etc., for describing multimedia sessions.

SIP defines different types of elements, which are user agents like user agent client (UAC) and user agent server (UAS), proxy servers, redirect servers, and registrar servers in its architecture. UAC creates a new request, and UAS generates responses respectively. In other words, when a software module initiates a request, it acts as a UAC for the duration of that transaction, and if it receives a request later, it assumes the role of a user agent server for the processing of that transaction. The proxy server helps to route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. Redirect servers are elements that support the location service by directing the client to contact an alternate set of user's URIs. The location service includes implementation of database which holds mapping information of a registered URI and other alternative user locations at which the user can be contacted. A registrar server processes Register requests to get the coming user's current contact location, which associates the agent's SIP or SIPS URI with the machine into which he is currently logged, for use by proxy servers, and this function supports personal mobility in which users can maintain a single externally visible identifier, regardless of their network location [4].

SIP allows an easy session setup process because of its simplicity. When a user agent (caller) initiates a call, it sends an *Invite* request, then the proxy server or redirect server transfers the request to the user agent server (the callee). If the user agent server receives the call, the response (*200 Ok*) message is sent to the caller, and when the *Ack* message is sent to the callee from caller, the session is established. Then the media session between the caller (UAC) and the callee (UAS) begins, and they send media packets using the format to which they agreed in the exchange of SDP. In general, the end-to-end media packets take a different path from the SIP signaling messages. The session ends by sending a *Bye* message when one of the user agents hangs up. Figure 2-1 shows the *Invite-Ack* transaction and the *Bye-Ack* transaction as processes of session establishment.

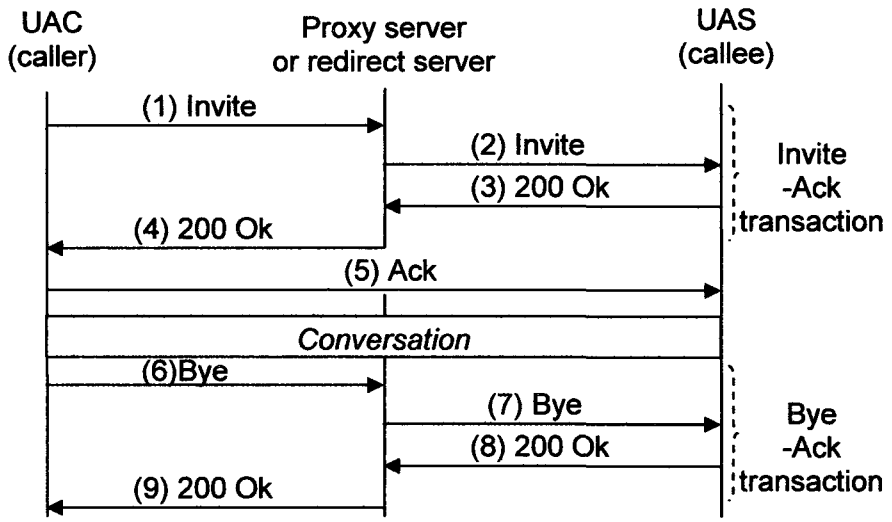

Figure 2-1 Flow of Session Establishment

The mandatory header fields in SIP are To, From, CSeq, Call-ID, Max-Forwards and Via. The To and From header fields show the originator and destination of the SIP request. Call-ID contains a globally unique identifier for the call, generated by the combination of a random string and the host name or IP address. The combination of the To tag, From tag, and Call-ID completely defines a peer-to-peer SIP relationship between the caller and the callee and is referred to as a dialog, which is identified at each UA with a dialog ID, which consists of a Call-ID value, a local tag, and a remote tag. CSeq or Command Sequence contains an integer and a method name. The CSeq number is incremented for each new request within a dialogue and is a traditional sequence number. Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop. A Via header field indicates the transport used for the transaction and identifies the location where the response is to be sent. Each SIP device that originates or forwards a message stamps its own address in the Via header field, usually written as a host name that can be resolved into an IP address using a Domain Name Service (DNS) query [31]. Each proxy uses the Via header field to determine where to send the response and removes its own address from the top. The header field contains the protocol name, protocol version, and a unique branch parameter that is used to identify the transaction created by that request and is used by proxies to detect loops. Also, a Via header field value contains the transport protocol used to send the message (such as TCP, UDP, TLS, and SCTP), the client's host name or network address, and possibly the port number at which it wishes to receive responses. The Jointly header fields, which are in addition to the mandatory request line and contains the method, Request-URI, and SIP version, contain addressing of messages, routing of responses, limiting message propagation, Ordering of messages, and unique identification of transactions.

Since the advent of the SIP, there have been many evolutions in SIP to provide more implemental architectures, to support service-user familiarity, and to provide an extensible framework. Figure 2-2 shows the brief history of SIP.

How to provide a reliable provisional response message by using the option tag 100rel and by defining the provisional response *Prack* method is suggested in the IETF RFC 3262, and how to allow a client to resolve a SIP URI into an IP address, port, and the transport protocol of the next hop to contact by using DNS procedures is suggested also. SIP can also use DNS to allow a server to send a response to a backup client if the primary client has failed, in the IETF RFC 3263. Specific Event Notification can provide an extensible framework by which SIP nodes can request notification from remote nodes indicating that certain events have occurred according to the IETF RFC 3265, and the *Update* Method allows a client to update the parameters of a session such as the set of media streams and their codec without changing the state of the current dialogue. This makes it very useful for updating session parameters within early dialogues according to the IETF RFC 3311.

RFC 3312 suggests an integration method of resource management by defining a generic framework for preconditions, which are extensible through IANA registration, and also discusses how network quality of service can be made a precondition for the establishment of sessions initiated by SIP. These preconditions require that the participant reserve network resources before continuing with the session. These preconditions simply require a participant to use existing resource reservation mechanisms before beginning the session.

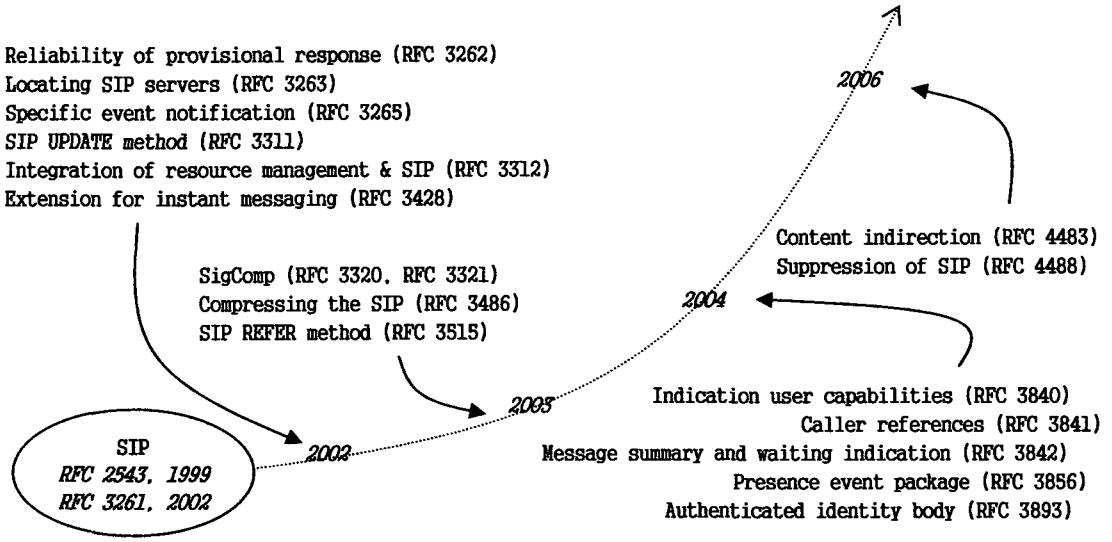

Figure 2-2 History of Session Initiation Protocol

Signaling Compression, whose architecture and prerequisites are outlined in the IETF RFC 3320 and which improves the compression efficiency compared to using simple per-message compression in the IETF RFC 3321, also supports SIP. The IETF RFC 3485 defines the Static Dictionary for the Signaling Compression of SIP and SDP that maybe used in order to achieve higher efficiency. The IETF RFC 3486 describes a mechanism to signal that compression is desired for one or more SIP messages, and also states when it is appropriate to send compressed SIP messages to a SIP entity.

Some SIP extensions define more methods such as *Message* and *Refer*. The IETF RFC 3428 proposes the *Message* method, which inherits all the request routing and security features of that protocol, to allow the transfer of instant messages. The IETF RFC 3515 defines the *Refer* method, the refer event package and the Refer-To request header, and requests that the recipient Refer to a resource provided in the request. This extension

provides a mechanism allowing the party sending the *Refer* to be notified of the outcome of the referenced request. This *Refer* method automatically establishes a typically short-lived event subscription used to notify the party sending a *Refer* request about the receiver's status in executing the transaction requested by the *Refer*. As a preventive, the IETF RFC 4488 specification provides a way to prevent the automatic establishment of an event subscription and subsequent notifications using a new SIP extension header field that may be included in a *Refer* request.

The user agent can convey its capabilities and characteristics, as parameters of the Contact header field, to other user agents and to the registrar for its domain in the IETF RFC 3840. A caller can express preferences about request handling in servers, as the IETF RFC 3841 suggests. These preferences include the ability to select which Uniform Resource Identifiers (URI) a request gets routed to and the ability to specify certain request handling directives in proxies and redirect servers by defining three new request header fields, Accept-Contact, Reject-Contact, and Request- Disposition, which specify the caller's preferences.

Some events packages carry information of SIP message-waiting status and message summaries or subscriptions and notifications of presence. The IETF RFC 3842 defines a SIP event package that carries message waiting status and message summaries from a messaging system to an interested user agent. The IETF RFC 3856 describes the usage of the SIP for subscriptions and notifications of presence. Presence is defined as the willingness and ability of a user to communicate with other users on the network. Subscriptions and notifications of presence are supported by defining an event package within the general SIP event notification framework.

The IETF RFC 3893 provides a more specific mechanism to derive integrity and authentication properties from an authenticated identity body (AIB), a digitally-signed SIP

message, or message fragment. A standard format for such bodies is given in this document. The IETF RFC 4483 defines a mechanism for content indirection in SIP messages and defines an extension to the URL MIME External-Body Access-Type to satisfy the content indirection requirements for the SIP. These extensions are aimed at allowing any MIME part in a SIP message to be referred to indirectly via a URI, according to the document.

As described, with the powerful supports of various SIP extensions, providing of even more services that 3G market demands for is realizable with SIP network in near future.

2.4 Secure Mechanisms Supported by SIP

Security mechanisms can be built into the protocol itself, including different variations of HTTP authentication or secure attachments at the transport layer or at the network layer. One of the mechanisms at the transport layer is the IPsec, which uses the Encapsulating Security Payload (ESP) protocol, the Authentication Header (AH) protocol, and the Internet Key Exchange (IKE) protocol.

Some other security mechanisms can be built into the communication establishment process from the beginning of the session initiation. Authentication and authorization are important parts of the secure mechanism.

In the SIP, secure communications are used to reach the user, where the specific security mechanism depends on the policy of the domain. The SIP provides a secure URI, called a SIPS URI. A call made to a SIPS URI guarantees that secure and encrypted transport, such as TLS, is used to carry all SIP messages from the caller to the domain of the callee. SIP supports the security mechanism, whose main concerns are message integrity, confidentiality, and the authentication of messages and of the user. The mechanism consists

of authentication and encryption in connection with other Internet protocols such as HTTP, TLS or IPsec, and S/MIME.

The SIPS URI allows resources to specify that they should be reached securely [4], and it can be used as an address-of-record for a particular user. In the SIPS URI scheme, "tcp" and "sctp" are both valid, although UDP is not a valid transport for SIPS. The SIPS scheme may signify that each hop over which the request is forwarded, when used as the Request-URI of a request until the request reaches the SIP entity that is responsible for the domain portion of the Request-URI, must be secured with TLS according to [4].

The SIP provides user-to-user authentication and proxy-to-user authentication by allowing the application of the HTTP digest authentication scheme [16]. With the HTTP protocol, the user client agent sends a request to the server in the form of a request method, URI, and protocol version, followed by a message containing request modifiers, client information, and possible body content over a connection with a server. The digest scheme of HTTP is based on a simple challenge-response paradigm. With the digest authentication scheme, a UAS challenges the coming UAC by using a nonce value and investigates the response from the UAC by checking a checksum (whose default is the MD5 checksum) of the username, the password, the given nonce value, the HTTP method, and the requested URI. The *401 Unauthorized* message is used by a UAS or a registrar server or redirect server to challenge the authorization of a UAC, and the *407 Proxy-Authentication Required* message is used by a proxy to challenge an unauthenticated *Invite* request. The responses are accompanied by header fields such as WWW-Authenticate header and Proxy-Authenticate header for carrying challenges and credentials in the responses to *401 Unauthorized* and *407 Proxy-Authentication Required* respectively. Then the UAC resends the *Invite* request with a header field such as the Authorization header field or the Proxy-Authentication Header field,

which contain the UAC's credentials after sending Ack. A user agent server may include the Authentication-Info header field in a 2xx response to a request that was successfully authenticated using digest based on the Authorization header field. In this way, the Authentication-Info header field allows a user agent to authenticate a proxy server and provides mutual authentication with HTTP digest.

SIP supports hop-by-hop encryption, which relies on network layer security like IPsec or transport layer security like TLS [32] and end-to-end encryption through the S/MIME. End-to-end encryption of the SIP message body and certain sensitive header fields can be done, and hop-by-hop encryption to prevent an eavesdropping that tracks who is calling whom can be done. Transport or network layer security encrypts signaling traffic, guaranteeing message confidentiality and integrity by utilizing certificates. The certificates are used in the establishment of lower-layer security, and these certificates are used to provide a means of authentication in many kinds of architectures. In the PKI scheme, when an end user, who holds private key, publishes public key, the user builds public key into a certificate and has it digitally signed by a trusted Certificate Authority (CA) for the purpose of protecting the disclosure of the public key. The signed certificates are kept and managed by utilizing the CRL. A certificate typically includes the public key being signed, a name whose public key is being signed, a validity period, the location (URL) of a revocation center, and the digital signature of the certificate produced by the CA's private key.

TLS provides transport-layer security over connection-oriented protocols like TCP. When TLS is chosen as the transport, the two servers exchange and verify certificates for authentication. TLS is most suited to architectures in which hop-by-hop security is required between hosts with no pre-existing trust association after a certificate exchange. IPsec is a set of network-layer protocol tools that collectively can be used as a secure replacement for

traditional IP and is most commonly used in architectures in which a set of hosts or administrative domains have an existing trust relationship with one another. IPSec is usually implemented at the operating system level in a host or on a security gateway that provides confidentiality and integrity for all traffic it receives from a particular interface (as in a VPN architecture) [4]. IPsec can be used on a hop-by-hop basis with an IPsec profile describing the protocol tools that would be required to secure SIP, and it is useful in case the UA has a pre-shared keying relationship with their first-hop proxy server.

Also, SIP allows end-to-end encryption through the S/MIME [4]. SIP messages carry MIME bodies, and the MIME standard includes mechanisms for securing MIME contents to ensure both integrity and confidentiality. S/MIME provides the cryptographic security services such as authentication and data security by using digital signatures and encryption. Encrypted MIME bodies are signed with the private key of the sender, but bodies are encrypted with the public key of the intended recipient. Also, S/MIME certificates are used to identify an end user, and these certificates assert that the holder is identified by the user's address-of-record.

SIP can also be used for the distribution of public keys by configuring the UAC, which sends a request containing an S/MIME body that initiates a dialog or sends a non-*Invite* request by structuring the body as an S/MIME "multipart/signed" CMS SignedData body [4]. Then UAS validates the certificate, determines the subject of the certificate and compare this value to the From header field of the request.

2.5 Limitation of the Secure Mechanism in the SIP-Based Network and Passive Devices

As mentioned in the previous section, SIP can be implemented easily and securely with the help of other lower layer protocols like TLS and IPsec and with encryption and authentication protocols like HTTP and S/MIME on the IP network. However, in spite of its prevalence based on its simplicity and various support for integrity and confidentiality, the SIP mechanism still has severe security problems in the protocol itself and in the session establishment mechanism.

The full encryption of messages provides the best means to preserve the confidentiality of signaling and guarantees that messages are not modified by any malicious intermediaries. However, SIP requests and responses cannot be naively encrypted end-to-end in their entirety because message fields such as the Request-URI, Route, and Via need to be visible to proxies in most network architectures so that SIP requests are routed correctly. Proxy servers still need to modify some features of messages, which are Request-URI, Via, Record-Route, Route, Max-Forwards, and Proxy-Authorization (such as adding Via header field values) in order for SIP to function. Proxy servers must therefore be trusted, to some degree, by SIP UAs for proper SIP functioning. For this purpose, low-layer securities for SIP are recommended, which encrypt all of the SIP requests or responses on the wire on a hop-by-hop basis and that allow endpoints to verify the identity of proxy servers to whom they send requests. TLS is connection-oriented transport layer protocol, and TLS is hop-by-hop security when there is no pre-existing trust association between hosts.

Hop-by-hop encryption preventing eavesdropping that tracks who is calling whom can be done, but the proxy server can still see who is calling whom, although the hop-by-hop encryption of Via fields to hide the route a request has taken ([4], [5]). Therefore, the confidentiality is not ensured perfectly, and the network needs a more secure mechanism to protect the confidential information from being announced to the public through spoofing or

eavesdropping by unauthorized parties and from replay attacks [33]. In addition, hop-by-hop encryption by IPsec is useful only between the UA and the first hop proxy server.

The actual security problems are related to the announcement of important information, which should be protected from malicious user agents through header fields. For example, the Call-ID header field shows the caller location, and the server response-header field contains information about the software used by the user agent server to handle the request. Also, the Via header field and the User-Agent header field reveal the path taken by the request and the methods used, as [4] documents, and the SIP message body may carry private information that should be kept confidential.

To utilize the SIPS URI, mutual TLS authentication needs to be employed. A client should have a certificate to allow mutual authentication. If not, TLS can be used in conjunction with another authentication mechanism. Also, certificates received in the authentication process should be validated with root certificates held by the client. Because there is no unique certificate authority, some limitation is unavoidable. However, users need to acquire certificates from well-known public certificate authorities, or users may create self-signed certificates. Pre-configured certificates between all SIP entities may be implemented when a previous trust relationship exists. However, the holder of a certificate should publish their certificate in any public directories as appropriate. Similarly, UACs should support a mechanism for importing manually or automatically certificates discovered in public directories corresponding to the target URIs of SIP requests.

[16] requests that a server need to check that the URI in the request line and the URI included in the Authorization header field point to the same resource. In a SIP context, these two URIs may refer to different users due to forwarding by some proxy. Therefore, in SIP, a server may check that the Request-URI in the Authorization header field value corresponds

to a user for whom the server is willing to accept forwarded or direct requests, but it is said to be not necessarily a failure if the two fields are not equivalent. This poses another problem, because the server cannot be sure of the device's authority over the network.

When the S/MIME Key Exchange mechanism is implemented in the network, network configuration problems are expected, because only a few of the intermediary network elements can view and process the SIP messages in this mechanism. [5]

Regarding to the functionality of the proxy in the authentication process, proxies must be completely transparent regarding user agent authentication by origin servers. That is, they must forward the WWW-Authenticate and Authorization headers untouched. If a proxy that passes authentication headers to the next hop is transplanted by the third party to get session information like from whom and to whom, the session is not in safety.

In the session establishment mechanism, especially in the registration step, authorization and authentication are handled in SIP either on a request-by-request basis with a challenge/response mechanism or by using a lower layer scheme that uses TLS. Registration entails sending a Register request to a special type of UAS known as a registrar. A registrar acts as the front end to the location service for a domain, reading and writing mappings based on the contents of Register requests. This location service is then typically consulted by a proxy server that is responsible for routing requests for that domain. Generally, SIP authentication is meaningful for a specific realm, a protection domain.

Also, because location services are not required to provide a SIPS binding for a SIPS Request-URI, and although location services are commonly populated by user registrations, when queried for bindings, a location service returns its contact addresses without regard for whether it received a request with a SIPS Request-URI.

Table 2-2 is the summary of some limitations of secure mechanism SIP supports.

Table 2-2 Secure Mechanism Limitations in SIP

Features	Limitations
HTTP Digest Authentication	▪ Offers protection of the Request-URI and the method of a message, but not for any of the header fields ▪ Within the scope of realms ▪ Digest is valuable when a user wants to authenticate themselves to a resource with which they have a pre-existing association ▪ Is one-way authentication
TLS Authentication	▪ Only over TCP ▪ Strictly hop-by-hop security ▪ Does not allow clients to authenticate proxy servers to whom they cannot form a direct TCP connection ▪ A UA that sends requests over TLS to a proxy server has no assurance that TLS will be used end-to-end.
IPsec	▪ Good only for UAs that have a pre-shared keying relationship with their first-hop proxy server ▪ IPsec profile is required
S/MIME Key Exchange	▪ The lack of a prevalent public key infrastructure for end users ▪ Susceptible to a man-in-the-middle attack with which an attacker can potentially inspect and modify S/MIME bodies ▪ The keys associated with S/MIME are most useful when associated with a particular user (an address-of-record) rather than a device (a UA).
SIPS URI	▪ The location service returns its contact addresses without regard for whether it received a request with a SIPS Request-URI.

IP devices like surveillance cameras are passive when they are compared with other network devices from a session-undertaking point of view. Passive network devices may have some major problems related to network security. The first problem comes from their passive characteristics. "Passive" means that devices should be and can be controlled and managed by other agents in the network, not by themselves. Also, the device is passive from an information protection point of view, in contrast to aggressive acquisition of private data on IP network. The second problem comes from the fact that the devices are tamper-sensitive. Anyone who knows the IP address of the device can tamper with the device and the private information on the IP network. The third problem is the issue of the management architecture of passive devices. Most passive devices have no functions like authentication, authorization, and audit abilities, which can give us more controllability over the devices.

In a SIP-based IP network, which especially includes passive devices preserving the confidentiality and integrity of messaging, preventing replay attacks or message spoofing, providing for the authentication and privacy of the participants in a session, and preventing denial-of-service attacks are security functions. Moreover, SIP message bodies also separately require the security services of confidentiality, integrity, and authentication to protect private information from such kinds of attacks.

The static password used for authentication with a digest user name is also regarded as a weak authentication, because there are many attacks like dictionary attacks and stealing passwords. A user name for authentication can be easily revealed in public, and then the password is the only method to ensure user's identification. For that reason, the administration that uses a better scheme for passwords is needed.

Authentication is a kind of proof process of identity between entities. Authentication can be established in one-way or two-way in case both parties need to be identified to each

other. When an agent is going to access the predefined network or a device is going to be installed into the network that has to be protected from an unauthorized third party, the authentication processes for each process are needed. These are access authentication and device authentication. After assurance of the agent or device, the network management can grant them authorities. This is another process of the secure mechanism, and it is called authorization. SIP entities, which include accessing users and passive devices, have to identify one another in a secure fashion. When a SIP endpoint asserts the identity of its user to a peer UA or to a proxy server, the identity should in some way be verifiable. In the mutual authentication scheme, the opposite direction, which means a proxy server or the peer UA provides its identity to the SIP endpoint, also needs to be verified.

In the PKI scheme, a certificate includes a private key of the vendor (which is usually of CA) and a public key, and the certificate is given to give a predefined right to the user. Also, a public key is combined with a user password in the PKI scheme. A "static" password ("static" is used to make the meaning of a "dynamic" password clear in this thesis, as a word with the opposite meaning.) also could be stolen easily, and even more, if it is of a passive device, the impact is beyond imagination.

Eventually, device management functions such as "access authentication", "device authentication" and "device certificate" are essential to enhance the network security for passive network devices.

Chapter 3

AAA SIP Server

In this thesis, some mechanisms to support weak SIP-based networks for passive device deployment are suggested. The first mechanism is to strengthen the authentication and authorization mechanism by utilizing a certificate and dynamic password for users and devices and by inserting AA servers and AADBs as intermediary network devices.

In a SIP-based IP network with passive devices, we may consider two possible session establishment processes. The *Invite* request by the predefined network user is one, and the *Invite* request by a passive device is another case. For the first case, when a user wants to establish a dialogue with passive devices or registers itself with the predefined network, its UAC sends an *Invite* request. When a server in the domain receives the request, the server identifies itself to the UAC and is forced to present the identity of the UAC in the mutual authentication scheme, and which means the user needs to go through an access authentication. For the second case in which a passive device is the UAC, the user agency is the UAS. The passive device would send a *Register* request every time it is deployed in the system and starts its own function or service, especially for the registration status. Maybe we

need to assume that the device is programmed with a fixed (but adjustable later) destination IP and port address. In this case, there are few possibilities that the device is controllable or accessible by the third party directly by changing the destination IP to send the private information to their location or by changing the device location to steal a private life. So we need to provide a way to protect the device from being used for unintended purposes. A device certificate can be a solution for this.

In common SIP usage, after the first authentication with a static password and user ID, the end entities keep static passwords during the initiated session lifetime and also keep the password for the end entities' lifetime. For the reason that one static password can be stolen by other users who do not have pure intentions during a session or during a lifetime, we need a dynamic password scheme together with a device certificate for this authentication scheme.

In addition, the administrating server such as the authentication authorization audit (AAA) server, which administers all processes of authentication and authorization, is introduced. In section 3.1, the authentication server and authentication DB are introduced, and the device certificate, the dynamic password scheme and its application in the SIP-based IP network are introduced in sections 3.2 and 3.2, respectively.

3.1 AA Server with AADB

The IP network is an open network, so any capable network device or agency may have a right to be connected to it, regardless of its wholesomeness. Usually in the authentication process, the password and user ID are used to provide user information to an authentication server that has the shared same secret as the password to make sure that the calling user agent is the right party that has provided its information during access to the network.

For some reasons related to network security, predefined IP network systems with passive devices as its entities need to endow their entities with the classified rights of network access according to their own charter in the process of authorization. For instance, individual user agents may have different access authorities, i.e., the agent *A* has authority to access a passive device *a*, but the agent *B* may not have the same right. Similarly, the IP devices might have classified authorities with relation to their deployment location. A device *a* may be located in the subnet area A, but not in the subnet area B.

For the purpose of identifying and authorizing the accessing agent, the look-up table, which might be called the AADB, can be tabled with sets of credentials to prove the agents' identities and the agents' authority limitations are essential. Here, the authority limitation means that user agents may have different levels of authorities from each other and may have different allotted network devices to access with relation to the deployment location and the access level. The AADB is desirable to contain the device certificate information, which is introduced in the sections of *3.4, Device Certificate & Device Authentication.* Protocols like LDAP and X.500 specifications support the directory service, and Certificate Revocation List (CRL) in X.509 especially enables AA servers to have AADB for the purpose of authentication and authorization.

A SIP server may proxy, redirect messages, or work as a registrar in the SIP mechanism. The lookup database for registration and the lookup database for authentication-authorization may be utilized in similar ways. The registration lookup combined with the authentication-authorization lookups may provide a stronger authentication scheme in SIP-based IP networks with passive devices. The detailed scheme with these database lookups is given at the last section of this chapter. Figure 3-1 shows possible applications of registration lookup and authentication lookup for each server.

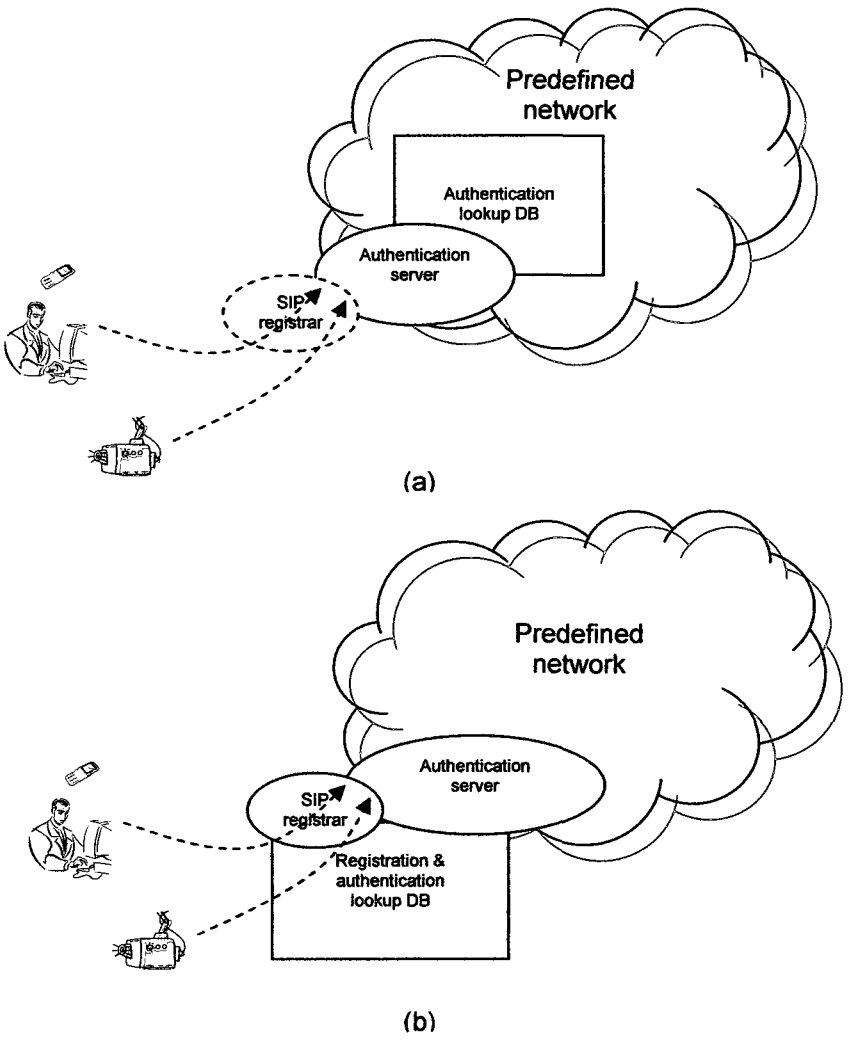

Figure 3-1 AA Server and AA Database

3.2 Dynamic Password

As explained in the previous chapter, the end-user agents that intend to access the secure SIP-based IP network need to be identified and be given access right through the authentication and authorization process. In the SIP protocol-based mechanism, one common

method of secure authentication is the HTTP digest authentication or TLS authentication by utilizing the user password and user ID scheme.

Here, the user's device and passive devices can be UAs of the passive IP network. When UAs initialize the service, the UAs send the *Register* message to a logical server in the server's domain, which is known as a SIP registrar, and when they are going to make a call after the initialization, the UAs send an *Invite* request with the user ID and password. During the initialization process, the UAC identifies itself using its address-of-record and password, which are known for the domain to the SIP network server, and updates its contact address. In the mutual authentication scheme, of course, the receiving SIP registrar or SIP proxy server needs to identify itself to the coming UAC, in similar way.

In a password-based public key scheme, the password is used to retrieve or use a private key. The user Id, which is the public key of a certificate in the PKI scheme, is the address-of-record in SIP. The digital signature is used to give confirmation of the user's identity in the certificate, which is signed by a CA. In this thesis, private keys are located in the remote database server to support the dynamic password scheme, and the passwords for retrieving the private keys are generated and are newly given whenever UAs are authenticated and are authorized. The figure below explains the mechanism of authentication and authorization by utilizing the dynamic password scheme.

Figure 3-2 shows the simplified authentication process in which a SIP registrar that has registration and authentication lookup in its database does the authentication process, and the mechanism that a private key stored in the remote server supports the dynamic password mechanism also is shown in the following processes:

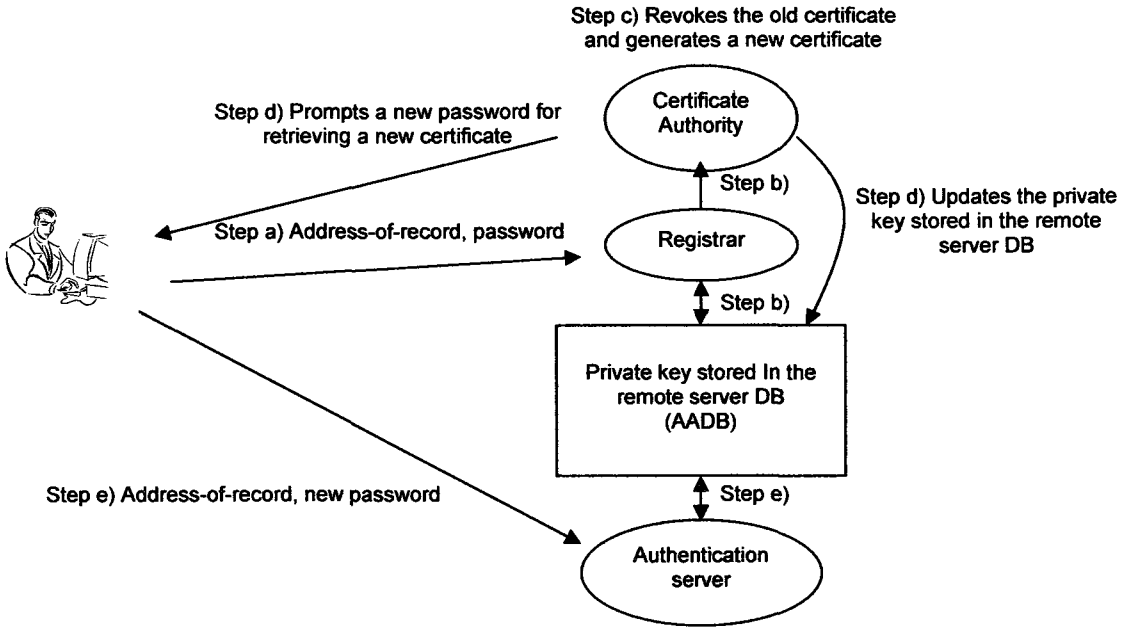

Figure 3-2 Dynamic Password and Authentication

a) The UAC sends a *Register* message to the registrar server with address-of-record and password;

b) The registrar looks them up in the database to retrieve the matching private key and validate the key with the certificate authority (Here, the CA can be located at the same server as the registrar);

c) The CA revokes the old certificate and generates a new certificate; At this moment, the Certificate Revocation List with the Password Revocation List is used;

d) The CA prompts the user to generate a new password to be used for retrieving a private key from the AADB, or the CA may generate one password when it revokes

an old certificate and generates a new one; At the same time the new password is generated, the CA updates the user's private key, which is stored in the database;

e) With the new password, the authentication server validates the UAC's certificate; if the password is stale (out of date) or unregistered, the authentication server sends an *Authentication failed* message to the agent.

The dynamic password and authentication scheme shown in figure 3-2 is demonstrated as shown below in figure 3-3. The dynamic password is used as a key for retrieving the registering user agent's certificate from the AADB and is compared with the password kept in the mapping table. When the UAC is authenticated, the registrar generates a new certificate and corresponding password, stores the certificate and the password in AADB tables, and endows the new password, which is a key to be used for future authentication, to the authenticated UAC with an *Ok* response. When the UAC intends to access the IP device to get information by sending an *Invite* request, the AA server consults the AADB to investigate the coming UAC's identity and gives the right to access the destination IP device for the authorized UAC.

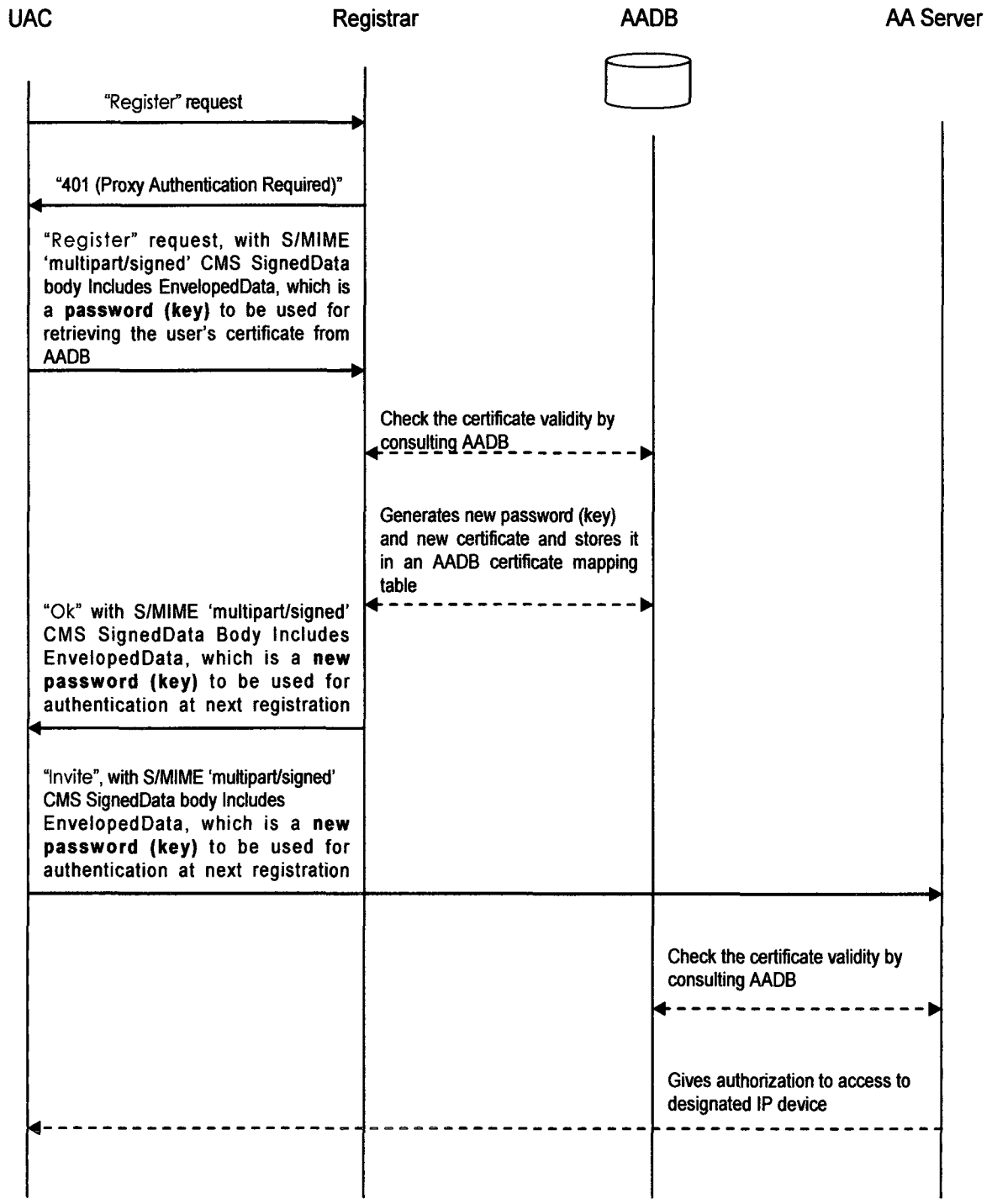

Figure 3-3 Dynamic Password Authentication Flow

3.3 Access Authentication by HTTP Digest

The SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP [16]. In the SIP, a UAS, registrars, and redirect servers make use of the *401 Unauthorized* responses to challenge the identity of a UAC. Instead, proxies may use the *407 Proxy Authentication Required* responses. The requirements include the proxy-authenticate, proxy-authorization, WWW-authenticate, and authorization in the messages. Since the SIP does not have the concept of a canonical root URL, the realm string alone defines the protection domain, and for digest authentication, each such protection domain has its own set of usernames and passwords.

Let's assume a SIP server has the authentication database that consists of registered users (That means the user has the authority to access the passive device.) information and registered devices (That means the device has the certificate, which is introduced in the later part of this chapter, to be inserted into the network.), and information like IDs and passwords. As the SIP server checks the sender's SIP address in the routing process, the server can identify and authorize the caller to contact with called device.

Figure 3-4 shows the access authentication scenario. Let's assume that the server has the authentication database and the record of the list of accessible authorized agents to each IP device. When the UAC desires to be connected onto the IP network and starts the session log-in, the following lists the operational steps:

a) the UAC sends an *Invite* request;

b) then a SIP proxy server (or a SIP registrar) responds with *407 Proxy Authentication Required* (or with *401 Unauthorized*);

c) The UAC sends the ID and password for realm A;

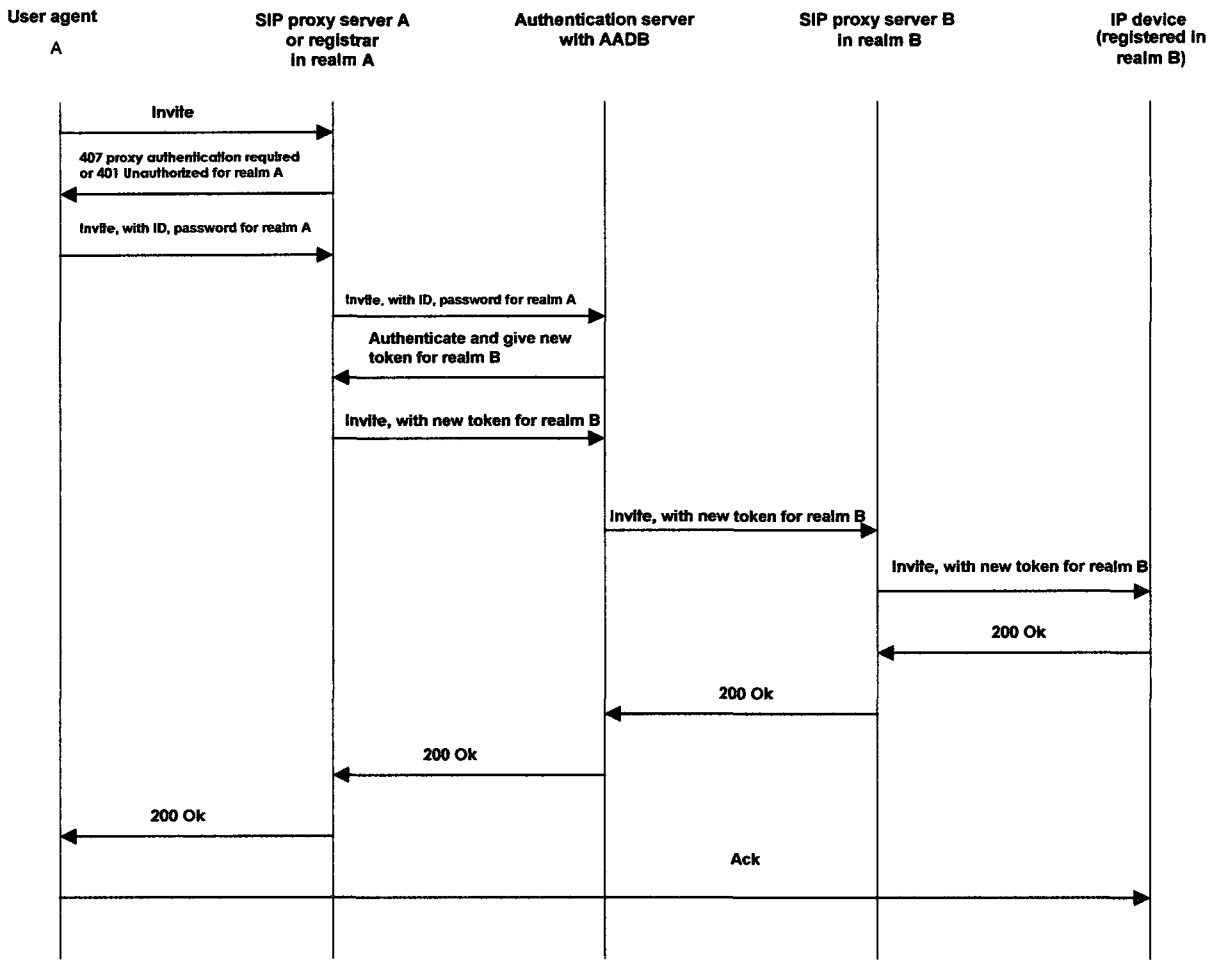

Figure 3-4 Access Authentication with HTTP

d) The SIP proxy server transfers the *Invite* message with the proxy authentication header field, which contains user's ID and password for the AA server;

e) The AA server retrieves the caller's record from its AA database with basic information about the caller. If no record exists, it then responds with the *403 Forbidden* message;

f) Otherwise, the AA server gives a new token for realm B, which is the protected domain for passive IP devices. At the same time, the administrator can add this new authorized user to the list of authorized users of the device;

g) Now the agent is granted access to the network, and the UAS generates another *Invite* message and sends the message with the given specified configuration as a token;

h) A proxy server in realm B recognizes the *Invite* message accompanied by the configuration and passes the message to User Agent Server which may be a passive IP device;

i) The UAS of called side rings and sends *200 OK*;

j) The caller server sends an *Ack* message.

As a result, the session can be established securely between the registered IP devices and the authenticated agent through the intermediate authentication server.

3.4 Device Certificate and Device Authentication

The process of identifying and authorizing the agent that intends to access the network has been called access authentication in this thesis. Now the concept of device authentication is going to be introduced. Let's assume that user A is an authorized agent and wants to get the information that the IP devices have and wants to manage the network by making good use of the information that the IP devices have, and the device is located in a specific region. In addition, as is usual with network devices, the IP devices can be located within the network boundary and can be removed from the network from the management point of view. Now,

the authorized management agent should know about the connectivity whenever the device is connected to the network and the location of the device. For this, the IP device should have some functions that are related to the authorization and the identification. One functional block will automatically provide its ID and password whenever it is connected to the IP network, and they would be presented at the registration process.

The access authentication itself does not provide any protection from device tampering. Therefore, there is still some possibility that an unauthorized third party could replace the existing device with their own device, control those devices, and steal the private information from the network. Moreover, the IP address or the SIP address as a device's identity is not satisfactory from the viewpoint of network security, because they are commonly published on the network during communication. For these reasons, passive devices should be managed by a certain administrative approach that includes the management of device identity and authentication using device identity authentication.

When we consider the hardware characteristics and network functionalities of passive devices, the devices' identities should be defined by a non-modifiable physical ID. Every network device is given its own unique serial number at the time of manufacturing, and it cannot be changed for any purpose. The media access control (MAC) address of network interface cards (NIC) of individual network machines is a kind of manufactured serial number, and it is unique. When a device brings its unique identity is deployed into the IP network, the authentication server recognizes its identity and retrieves the device's record from its authentication database during the authentication process if the record of the device exists.

Nevertheless, the authentication server recognizes the identity of the upcoming network device, and the device must present its other credential attributes like public key, device

location, validate time period, and a set of registered managers. For the example of device location, the server should know the new physical location of the device within the network at the time of deployment and should check its legitimacy. For the example of validate time period, if the current time of new deployment is out of the validated time period boundary, the server should not permit the device to have access rights. Also, the set of managers assigned to the upcoming device should be announced to the server for the purpose of user agent authentication and certificate management.

When the password of a device is considered for access authentication, the static password associated with the passive device may easily be known to the other party so that they can eavesdrop and access the device illegally. The application of the dynamic password is a reasonable way of securing access to SIP-based passive devices. The authentication server could be used in the creation, allowance, and revocation of dynamic passwords as access tokens in order for the devices to be connected to the network after their identities are authenticated.

Therefore, one approach of authorizing the passive device is to grant a device certificate whenever the device is connected and is granted to access to the network dynamically. The certificate can be regarded as an authentication token to access the network for a passive device. In a case where the device has a standardized certificate, the authentication server may use a protocol like X.509 ([34], [35]) to determine whether the current status of the certificate of the device is valid. If the certificate is valid, the authentication server grants a new password in the same manner as the first approach of utilizing a unique serial number.

In addition to the granting of a device certificate, we can implement the AADB together in the process of authentication and authorization. An authentication-authorization

(AA) server grants the device access and endows it with a new device access password when the server is confirmed with the device identity, which includes all of the credentials related to the device after retrieving the AADB at the point of new deployment. Then a registered user (management) agent who wants to access the passive device should know the changed password to acquire the non-public information. The Server-based Certificate Validation Protocol (SCVP) [36] may be utilized for this purpose in the near future.

Here the authentication server may take the roles of authorization server together and the AADB, which was introduced in the previous chapter, might be used during this authentication and authorization process.

An example of a lookup table for device authentication is shown in Table 3-1.

Table 3-1 Example of AADB

Device ID (MAC address)	Password or Public Key (more than 8 digits)	Location Limitation (logical area)	Time Limitation StartDate/ End Date (yyyymmdd)	Assigned Managers (Agent ID)
02:A6:1F:CA:34:7B	aaaaaaaa	Section A	20071001/ 20081001	AGNT_A
02:A6:1F:00:EE:B5	bbbbbbb	Section A, C	20071201/ 20080530	AGNT_B, AGNT_C
02:A6:1F:00:EE:B5	cccccccc	Section B, C	20071201/ 20080530	AGNT_D
A1:B2:C3:D4:55:F6	dddddddd	Section D	20071001/ 20171001	AGNT_K
...	...	...	...	...

In the table, time limitation can be given according to the validity period of the device certificate. Also, this table includes some administration information that is needed. Password management may follow the dynamic password scheme when the IP devices have functional blocks such as a data read/write module for it.

Figure 3-5 shows the process of authentication and authorization between the passive IP network device and an authentication server by using AADB. The following lists the steps involved during the authentication and authorization process:

a) The UAC sends a Register message to the registrar server with an address-of-record, a password, and a device certificate;
b) The registrar validates the key and certificate with the certificate authority. The CA can be located at the same server as the Registrar;
c) If the certificate is validated, the CA revokes the old certificate and generates a new certificate. At this moment, the certificate revocation list with a password revocation list is used;
d) The CA generates and gives the IP device a new password to be used for authentication and updates the AADB authentication table;
e) With the new password, the authentication server validates the UAC's certificate. If the password is stale (out of date) or unregistered, the authentication server sends Authentication failed message to the agent.

Furthermore, in addition to the device authentication scheme with TLS, the same authentication scheme that is introduced in the previous section of *3.2, Dynamic Password,* can be utilized with the device certificate, as shown in the figure.

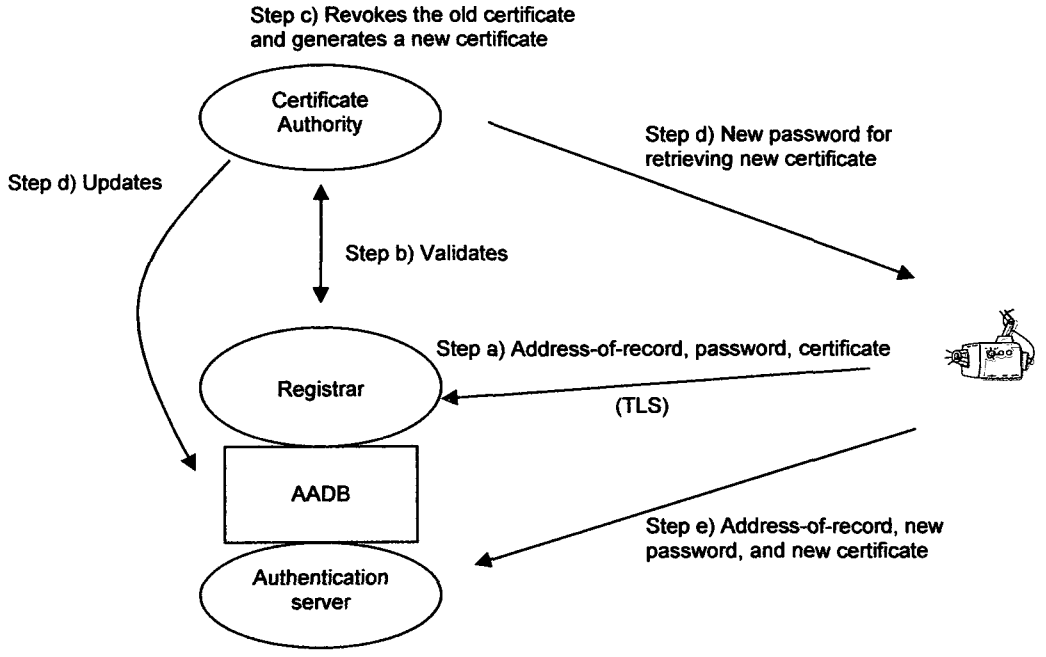

Figure 3-5 Device Certificate and Authentication

3.5 Authentication, Authorization, and Audit

Now, the concept of the authentication, authorization and audit (AAA) server is introduced in this section. In the preceding sections, we looked at access authentication and device authentication. Figure 3-6 shows the access authentication and device authentication in a SIP-based IP network. First, passive devices try to acquire device authentication and to be granted with authorization on the network. On the other hand, a user agent who wants to access the device tries to get the access authentication. The authentication server looks up the authentication database to identify the agent or devices and to check which agent has the authority of access to which device in the network. Also, the authentication server checks whether the incoming passive network device is permitted to be deployed into the defined

network boundary. If all authentication and authorization conditions are satisfied, then the user can access the passive device.

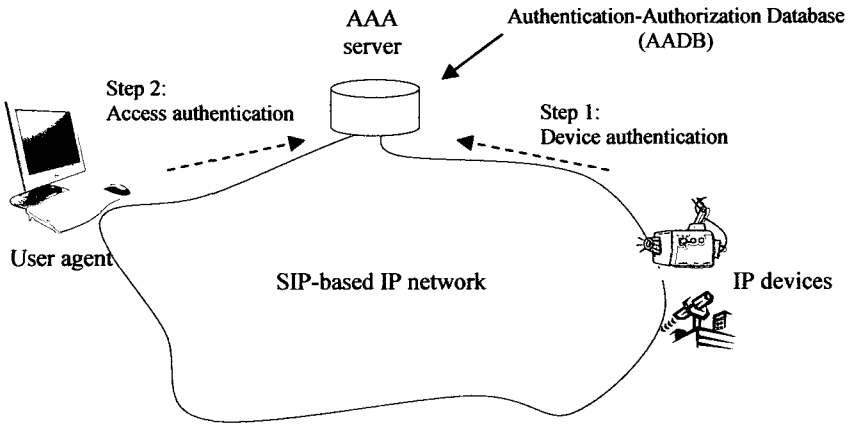

Figure 3-6 Access Authentication and Device Authentication

Here, the AAA server and the AADB work together to provide a more secure scheme in the SIP-based IP network which contains passive network devices like surveillance cameras accessing private information as its components. Furthermore, passive devices such as surveillance cameras access private information, which should be managed in an administrative way. Therefore, the access audit is another important factor to be considered in the design of the proposed architecture besides the protection of private information. The audit trail is needed so that the managing party may survey the time log and the access information from the record. Information such as "who has accessed which devices", "how long it lasted", and "which device has been deployed in which area" would be recorded. The proposed architecture of using an authentication server to control the network access of passive IP devices could meet the above audit requirement to record and provide the audit trail mentioned above.

Chapter 4

Access Authentication and Dynamic Session Key

In the first part of this chapter, access authentication by utilizing RADIUS server as the authentication server for user access and device access authentication is discussed, and the dynamic session key is introduced and discussed deeply to provide a more secure channel for exchanging messages, which includes encryption keys and passwords at the rest part. Moreover, how the asymmetric encryption and the dynamic session key work together to acquire a secure network in the SIP-based network is introduced in the dynamic session key mechanism.

4.1 Access Authentication with RADIUS

In the network service market, RADIUS is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server (NAS) that desires to authenticate its links and a shared authentication server [14]. In this chapter, the RADIUS server as an access authentication server is used to provide access control with SIP and to show the other possible method of access control.

Figure 4-1 shows the access authentication scenario. Let's assume that the server has the authentication database and the record of the list of accessible authorized agents to each IP device. When the UAC desires to be connected onto the IP network and starts the session log-in, the following list is the operational steps:

a) The UAC sends an *Invite* request;

b) Then a SIP proxy server responds with *407 Proxy-Authentication Required*;

c) The UAC then sends the ID and password;

d) The SIP proxy server transfers the user's ID and password to the Authentication server with an *Access-Request* message. The authentication server can be composed using a RADIUS server, for example. In the case where the architecture has a RADIUS server, the residing client server may send an *Access-Request* message to the RADIUS server, including authentication information like username (or device name) and password (the password should be a registered one);

e) The authentication server (or RADIUS server) retrieves the caller's record from its authentication database with basic information about the caller. If no record exists, it then responds with an *Access-Reject* message;

f) Otherwise, the RADIUS server wishes to issue a challenge to which the user must respond, and the RADIUS server sends an *Access-Challenge* response;

g) The client then re-submits its original *Access-Request* with a new request ID, with the user-password attribute replaced by the response (encrypted) and including the state attribute from the *Access-Challenge*, if any. When the server calculates the responding value, a one-way hash function may be used;

h) If all of the conditions are met, the list of configuration values for the user is placed into an *Access-Accept* response. At the same time, the administrator can add this new authorized user to the list of authorized users of the device;

i) Now the agent is granted an access to the network, and the UAS generates another *Invite* message and sends the message with the given specified configuration as a token;

j) The UAS recognizes the *Invite* message accompanied by the configuration and passes the message on;

k) The UAS of the called side rings and sends *200 OK*;

l) The caller server sends an *Ack* message.

As a result, the session is established securely between the registered IP devices and the authenticated agent through the intermediate authentication server, as shown in figure 4.1 above on the SIP-based network.

In figure 4.1, a token that is given to the caller may be one of the certificates or new passwords for the realm that the call has to be transported to. Here we can adopt the certificate authority scheme and the dynamic password concept to complement the shared secret mechanism in the RADIUS server authentication.

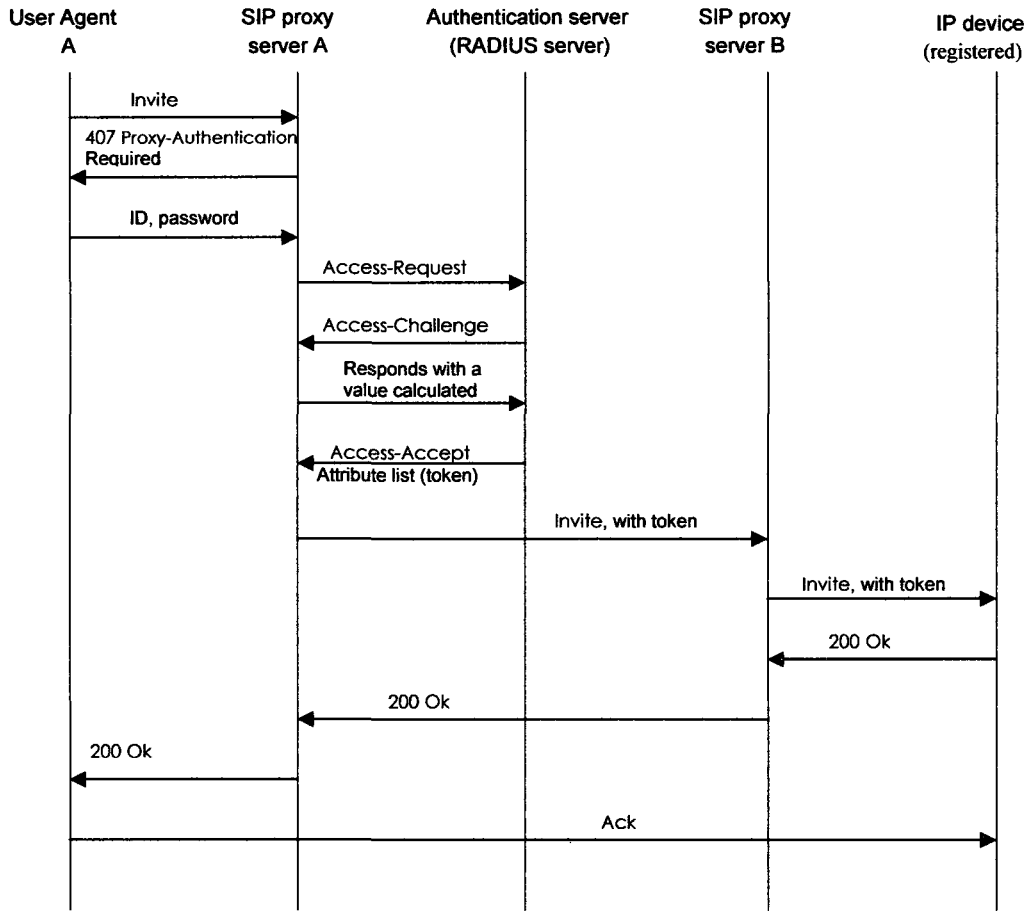

Figure 4-1 Access Authentication with RADIUS Server

4.2 Dynamic Session Key

As a precondition, the administration party must know the IP address and the device's serial number of any IP device that is going to be deployed in the protected area. To achieve this goal, the administration server needs to have any methodology to map the unique device identity and the assigned deployment location. Having an AADB is one solution for this, and when an IP device approaches to register to be deployed and connected to the protected

network area, the AA Server must retrieve the AADB to see whether the coming IP device is eligible to get a connection to the area after the first deployment, in which the device's legibility has been given by an administration person by entering the certified serial number of the IP device and its expected deployment location map.

A unique serial number is used as a shared secret together with the certified public key set at the beginning stage of the device authentication. This authentication scheme gives more security benefits than the single usage of the certified public key or serial number for registration.

The temporary session key, which is the public key and private key set, and the certified public key work together to provide secure session establishment in this architecture. The temporary key set is transferred after they are encrypted by the certified public key, and the temporary key set should be replaced with a new one every session by reporting to the AA server. Another advantage of this scheme is the future session key transporting process, because except for the first registration process, the server only needs to check the AADB for authentication of the IP device, whose tables keep enough information about the registered IP device. The only thing the IP device does when it requires a new session key is provide its identity, which is the registered private key.

4.2.1 Device Authentication

IP devices are managed by their unique serial number assigned at the manufacturing stage; moreover, the unique serial number of an IP device is used as a shared secret with the system administrator at the beginning stage of authentication. As soon as the device is authenticated by the unique ID, which is a device serial number, a new device authentication ID is generated. Therefore, IP devices are authenticated, authorized, and registered in a secure way.

Figure 4-2 shows the process of device authentication, which utilizes the PKI scheme and the device's unique serial number for the device registration in SIP. The following list is the steps the device authentication process:

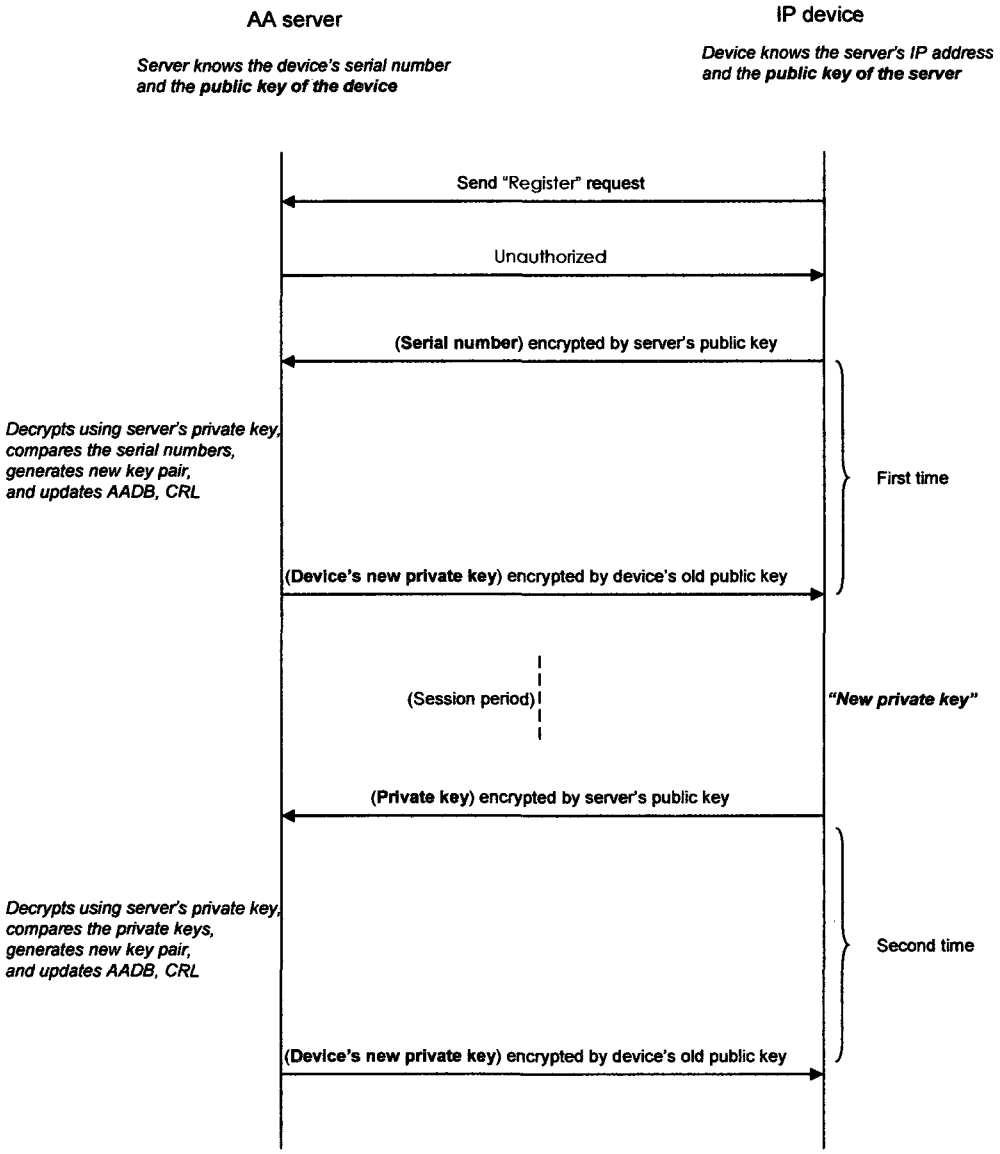

Figure 4-2 Device Authentication

a) The IP device sends a *Register* request;

b) The administration server responds with an *Unauthorized* response and the server's public key. (The server's public key may be stored in the device's dynamic memory device when the IP device is manufactured and certified. Then the server does not need to send its public key over the network, because it can be a vulnerable point for security attacks.);

c) Here the IP device should know of the server's public key, which should be registered, to see whether the server is the administrating one. After confirming the server, the IP device sends *Register* with its credentials, the IP device's unique serial number that is encrypted by the certified public key of the server;

d) The server decrypts the message body, which is the IP device's unique serial number, using the server's own private key. At the decryption stage on the server side, the administration person should be able to read the message body which contains the IP device's serial number, to confirm;

e) The server sets up AADB tables, the CRL, the location map, etc., with an administrator's help for only the first registration stage. The server might retrieve these tables to see whether the IP device has the privilege to be connected to the protected network later after this registration stage. The certificate revocation list is used to check whether the IP device's certificate is effective when the IP device is going to register for the protected area;

f) When approved, the AA server generates a new set of public-key private-key sets for the authenticated IP device and keeps the key set information in the AADB with the expiration time information. The key set is effective for a very short time period, so the IP device needs to renew the public key set by reporting at the end of every

session. The adjustment of the effective time period might need to be done according to the potential length of the SIP sessions;

g) The server sends an Ack response with the newly generated IP device's public key set, which is encrypted by the device's public key;

h) The IP device decrypts the message body using the device's own private key, which is going to expire, and gets and stores its own newly given public key set, which will be used as an asymmetric session key for a new session between the user agent and the IP device in future usage.

4.2.2 Dynamic Session Key Distribution

When a registered and authenticated user aims to establish a session with the IP device, the temporary session key for a session with the designated IP device that the user is going to access is given to the users in a secure way as shown in figure 4-3. The AA server that administrates the protected network area should know about the registered user in advance. For example, a mapping table of the AADB defines that user agent "*a*" who has certified public key "*A*" is able to establish a session with an IP device "@". The key distribution process is described below:

a) When a registered user agent sends an *Invite* message that designates the IP device's IP address (SIP address);

b) a proxy server redirects the message to the AA server, which administrates the IP device in the assigned area. Here the contact info of the IP device needs to be set up to follow the administration policy;

c) The AA server checks whether the user agent has the right to access to the IP device to establish a session. When the user has a right, the server sends the designated IP device's temporary public key, which is encrypted by the user agent's public key.

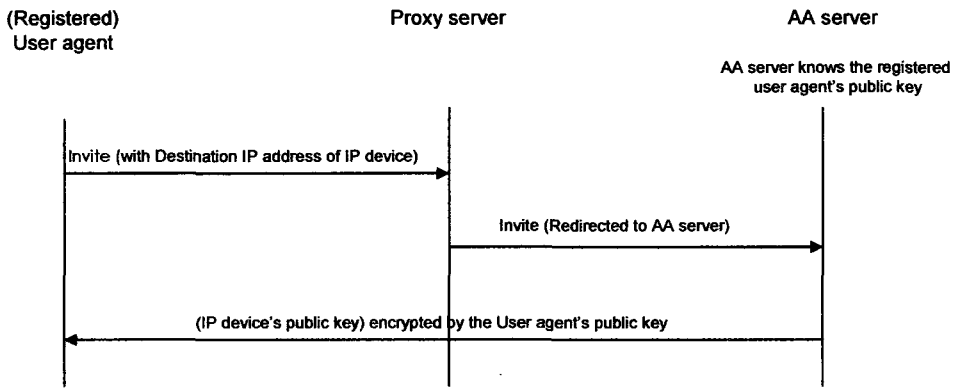

Figure 4-3 Session Key Distribution

4.2.3 Session Establishment

Any registered user that already knows the target IP device's public key can establish a session with the designated device, as explained below:

a) Then the user agent sends an *Invite* request that is encrypted by the IP device's public key, which is temporary and is valid for a given period;

b) The IP device decrypts the message using its own temporary private key which was given by the AA server after the last registration;

c) Then IP device sends an *Ok* message;

d) The user agent sends an *Ack* message, and then a session is established.

The temporary session keys, which are the public key and the private key, are valid for a session period so that the IP device is programmed to report after a session finishes and to acquire a new session key set. Here, the valid time period can be set up as an expiration time of the session key when the network system faces difficulty in the management of the deployed IP devices' connectivity.

Chapter 5

Comparison

5.1 AAA and RADIUS

In this thesis, some ways of constructing secure mechanisms in SIP-based IP networks by introducing the authentication method through an AAA server with an AADB, device authentication with device certification, and the concept of dynamic password were presented in the previous chapters. This chapter presents comparisons between the AAA server and the RADIUS server for the authentication mechanism and their features of security.

As explained previously, access authentication and device authentication with a device certificate by the AAA server with an AADB provide extended network security from the beginning of the network access trial by end entities in terms of network protection, which filters unidentified and unauthorized users that have possibilities of doing harms to the predefined network domain through some attacks, which are explained in Chapter 1. The RADIUS server also provides similar protection to the AAA server's except for the fact that it can only support the authentication for active end entities, not for passive devices which do

not have the flexibilities of identification and non-public information protection abilities which are essential to the SIP-based IP network.

Next, from the viewpoint of confidentiality, the above fact can also be said in other words; that is, the AAA server has the ability to provide confidentiality through the mechanism of dynamic password management, because the static password, which is weak against dictionary attack schemes, is not used in this mechanism anymore. This dynamic password scheme can make the dictionary attack weaken by changing passwords whenever the end-user agent gets an access right to the predefined network. Unfortunately, the authentication with the RADIUS server does not deal with password management, and there is no way of replacing passwords after one user agent has a shared secret in the RADIUS system. Even in the case of a stolen password, the dynamic password scheme is stronger, and the AAA architecture supports it.

Thirdly, the RADIUS server needs to have a shared secret with the coming agent for the authentication of the agent, but the AAA server does not require a pre-shared secret, even for passive devices coming, because it can utilize the PKI scheme for authentication.

Fourthly, the RADIUS server needs another network intermediary device like the NAS as a client of the RADIUS server, which has the responsibility of passing messages to its designated RADIUS server, and contrary to the fact, the AAA server does not need to have extra servers for the authentication process. That means we can have a simple and cost-saving secure network for SIP, and the system may stay in a robust state without having any intermediary machines, which may cause system malfunctioning when the machine is out-of-order.

One of the other differences between the two servers is available protocols such as the transport protocol. The UDP has to be used for RADIUS for technical reasons [14], and for

the SIP, both UDP and TCP can be chosen. When UDP is chosen for SIP, the SIPS scheme cannot be used. As explained, there are some limitations in using the RADIUS server as an authentication server in terms of the availability of protocols.

The summary of the comparison between the two servers, which are shown as authentication servers, is given in the table 5-1.

Table 5-1 Comparison of the AAA Server and the RADIUS Server

Authentication Server / Features	AAA Server with AADB	RADIUS Server
Authentication of passive devices	Yes	Yes (partially)
SIPS scheme	Yes	No
PKI scheme	Yes	No
No extra server required	Yes	No
No shared secret required	Yes	No

As shown, with consideration of security features, it is obvious that the AAA server with an AADB provides a stronger secure mechanism, even though the RADIUS server supports the authentication of passive devices with some help from the dynamic password scheme in the authentication process. Therefore, for a secure network system in a SIP-based area, the AAA server with an AADB can be recommended strongly.

5.2 Static and Dynamic

Dynamic password scheme and dynamic session key scheme were introduced in previous chapters. Here static method and dynamic method is compared. As we expect from the

original meaning of the word, static passwords or static session keys have a longer life cycle than dynamic ones do. The longer life cycle of a password makes it more convenience for users to remember, but it gives more chances for outside attacks like dictionary attacks and replay attacks. More frequent replacement provides more safety, but we need to find the proper frequency of the dynamic password or session key according to the system characteristics, because too frequent changing increases the network system load and decreases system efficiency in network transportation.

For the dynamic password mechanism, when a user agent registers, the network service provider prompts the coming user to change the password for retrieving the private key, which is stored in the AADB after initial authentication. This time period that the registered user keeps the connection might be considered longer if we compare the time to the dynamic session key life cycle. For the reason that the dynamic session key needs to be changed at every session, the changing of the session key can be regarded as more frequent and safer.

In addition, when the network system requires a more secure dynamic mechanism, the "expiration" time of the dynamic password or session key can give more flexibility to those dynamic duration adjustments.

Chapter 6

Conclusions

Passive IP devices like SIP-based surveillance cameras need to be secured due to the private information that they may transmit. Architecture to secure the private information that the device could access in a peer-to-peer overlay network is proposed.

This architecture uses an authentication server to provide the security mechanism for AAA services and access control. It combines the security features of authentication servers with the SIP architecture to provide AAA services to register users needing access to passive IP devices.

The dynamic password mechanism and dynamic session key mechanism for authenticating the accesses of the passive devices managed by the authentication server are also proposed to enhance the security features of devices. Moreover the dynamic mechanism gives the passive devices deployed network management a stronger control way than the static mechanism does for the SIP-based network.

Also, all users in this infrastructure would have one or single authentication credentials if an organization stores its user database in a LDAP database. All information processing systems can use such an LDAP database for user authentication and authorization, which in

turn means the single sign-on features have been achieved. In addition, single AADB helps the network administration of users and devices by assisting the user access control and device deployment for the SIP-based IP network.

Nevertheless, there are a few concerns to be resolved about the applications in the field. First of all, there are no standardized device certificates. Recently, companies like Cisco, Sun, and Novell have started to give certificates for networking hardware devices and systems, but the next step of the network working group still needs to enhance the compatibility of passive network devices by unifying industry device certificate standards with the different applications of device certificates. The second concern involves the key distribution policy and assignment of privilege of key revocation. There can be two methods in managing the dynamic password mechanism. One way is to have the authentication server "push" a new key to the coming UA. The other way is to make it a policy that the user needs to generate a new key whenever access is attempted.

Currently, the PANA working group has just come out as a protocol for the IP-based network access authentication protocol. PANA defines a new Extensible Authentication Protocol (EAP) lower layer that uses IP between the protocol end points, and the document says that upon following a successful PANA authentication, per-data-packet security can be achieved using physical security, link-layer ciphering, or IPsec. Through the support of PANA, a SIP-based IP network may provide a more intensive mechanism for passive IP devices. The PANA will be discussed for its application in the SIP-based network as one of the authentication mechanisms as a future work, and its pros and cons for the network will be discussed deeply when the protocol jumps into the network market applications.

Bibliography

[1] D. L. Shinder, *Computer Networking Essentials*. Indianapolis: Cisco Press, 2002, p91.

[2] R. Fielding, J. Gettys, J. Mogul, H. FryStyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol—HTTP/1.1," IETF RFC 2616, June 1999.

[3] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka, "S/MIME Version 2 Message Specification," IETF RFC 2311, March 1998.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handly, and E. Schooler, "SIP: Session Initiation Protocol," IETF RFC 3261, June 2002.

[5] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol," IETF RFC 2543, March 1999.

[6] P. Mehta and S. Udani, "Voice over IP Sounding good on the Internet, IEEE Potentials," October/November 2001, pp. 36-40.

[7] International Telecommunication Union, "Packet based multimedia communication systems," Recommendation H.323, July 2003.

[8] G. Camarillo and M. A. Garcia-Martin, *The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the Cellular world.* Chichester: John Wiley & Sons Ltd, May 2006.

[9] K. Singh and H. Schulzrinne, "Peer-to-Peer Internet Telephony using SIP," in *Proceedings of the international workshop on network and operating systems support for digital audio and video,* Washington, USA, 2005, pp. 63-68.

[10] Skype Ltd., Skype. Take a deep breath, http://www.skype.com.

[11] Vicon Industries, Inc., Getting the Most from Emerging IP Video Technology, *White Papers*, http://www.vicon-cctv.com.

[12] A. Neon-Garcia, I. Widjaja, Communication Networks: McGraw-Hill Higher Education, 2000, p 718.

[13] U.S. Department of Commerce, "Digital Signature Standard (DSS)," FIPS PUB 186-2, January 2000.

[14] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial-In User Service (RADIUS)," IETF RFC 2865, June 2000.

[15] S.-I. Sou, Q. Wu, Y.-B. Lin, and C.-H. Yeh, "Prepaid Mechanism of VoIP and Messaging Services," *ITRE*, 2005, pp. 255-259.

[16] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication," IETF RFC 2617, June 1999.

[17] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 3280, April 2002.

[18] S. Kent and R. Atkinson, "Security Architecture for Internet Protocol," IETF RFC 2401, November 1998.

[19] W. Polk, R. Housley, and L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation Lists (CRL) Profile," IETF RFC 3279, April 2002.

[20] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke, "A Security Architecture for Computational Grids", in *Proceedings of the 5th ACM Conference on Computer and Communications Security*, 1998, pp. 83-92.

[21] S. Tuecke, V. Welch, D. Engert, L. Pearlman, and M. Thompson, "Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile," IETF RFC 3820, June 2004.

[22] M. Parthasarathy, "PANA Threat Analysis and Security Requirements," IETF RFC 4016, March 2005.

[23] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy, and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA) Framework, " IETF RFC 5193, May 2008.

[24] J. Ma and M. A. Orgun, "Specifying Agent Beliefs for Authentication Systems," in *IEEE Proceedings of ECUMN'07*, 2007, pp. 410-418.

[25] M. Burrows, M. Abadi, and R. M. Needham, "A Logic of Authentication," in *ACM Transactions on Computer Systems*, vol. 8 (1), 1990, pp. 18-36.

[26] S. W. Jung and S. Jung, "Secure Password Authentication for Distributed Computing," in *Computational Intelligence and Security, 2006 International Conference*, vol. 2, November 2006, pp. 1345-1350.

[27] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," IETF RFC 1510, September 1993.

[28] B. Schneier, *Applied Cryptography*, 2nd edition, Wiley, 1996.

[29] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," IETF RFC 4120, July 2005.

[30] H. Liu and P. Mouchtaris, "Voice over IP Signaling: H.323 and Beyond," *IEEE Communications Magazine*, October 2000, pp. 142-148.

[31] A. B. Johnston, *SIP: Understanding the Session Initiation Protocol*, Artech House Publishers, 2004.

[32] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," IETF RFC 2246, January 1999.

[33] Cisco Systems Inc., "Security in SIP-Based Networks," *White Papers*, 1992-2002

[34] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," IETF RFC 2560, June 1999.

[35] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF RFC 3280, April 2002.

[36] T. Freeman, R. Housley, A. Malpani, D. Cooper, and W. Polk, "Server-based Certificate Validation Protocol (SCVP)," draft-ietf-pkix-scvp-32, work in progress.

[37] J. J. Kong, D. Lou, and T. Yeap, "Security System for Passive IP Devices on SIP based Network," in *IASTED Proceedings of Communication Systems, Networks, and Applications*, October 2007.