인터넷 서비스 감청을 위한 ETSI 표준기술

김성혜* 박소영* 강신각**

현재 인터넷을 통하여 다양한 형태의 새로운 서비스들이 빠르게 등장하고 있다. 인터넷 서비스의 다양성과 편리성 때문에 많은 사람들이 인터넷을 통신 수단으로 활용하고 있다. 합법적 감청은 공공안전과 국가보안의 확보를 위해 필요하다. 최근 인터넷 사용의 증가로 인터넷을 이용한 통신에 대해 합법적 감청이 필요하게 되었다. 현재 ETSI 에서는 인터넷 서비스에 대한 감청 표준을 진행하고 있다. 인터넷 감청 표준화를 위해 인터넷의 특성에 따른 감청 표준의 정의가 필요하고 인터넷을 이용한 다양한 형태의 응용 서비스에서도 감청 표준이 필요하다. 본 고는 ETSI 에서 표준화되고 있는 인터넷 서비스의 감청 기술에 대해 설명하고 현재 인터넷관련 합법적 감청 기술 표준화의 동향에 대해 살펴본다. ▨

목 차

* ETRI 융합통신표준연구팀/선임연구원
** ETRI 융합통신표준연구팀/팀장

Ⅰ. 서 론

국제 감청 표준은 유럽의 대표적인 표준 단체인 ETSI(European Telecommunication Standards Institute)의 TC-LI(Technical Committee-Lawful Interception) 서브워킹그룹에서 가장 활발히 진행되고 있으며 ETSI 감청 표준은 유럽 국가뿐만 아니라 미국, 호주, 중국 등의 다양한 국가에서의 적극적인 참여로 개발되고 있다. 합법적 감청 제도가 도입된 많은 국가에서 ETSI 표준에 의거한 감청 표준을 채택하고 있다.

ETSI TC-LI 에서는 감청 기술 자체에 대한 전반적인 표준과 인터넷과 관련된 감청 표준을 정의하고 있다. 감청 표준은 이동통신 서비스에서 표준화된 감청 기술의 필요성으로 시작되었는데 현재 인터넷에서도 감청의 필요성이 높아 인터넷 감청 표준 개

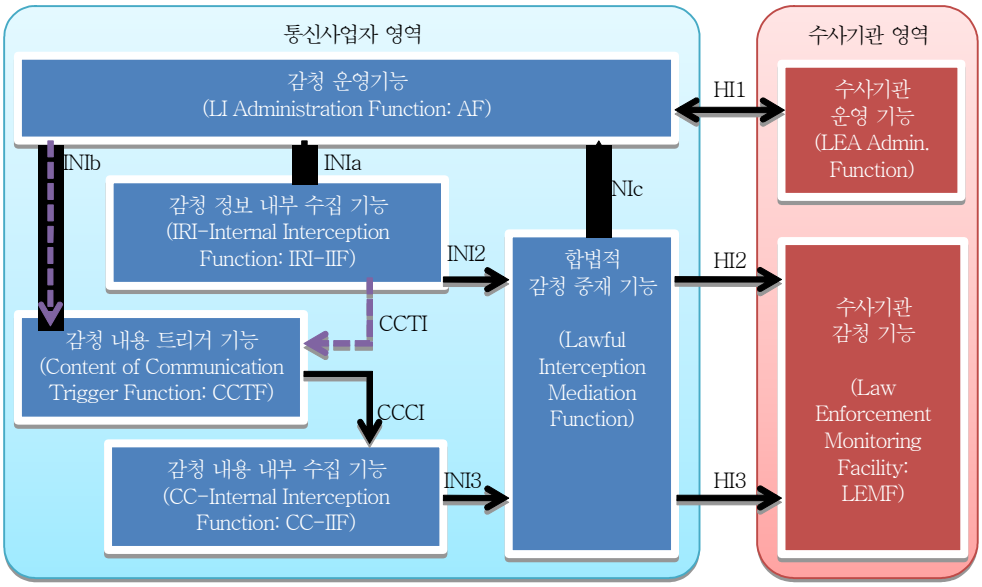
발이 진행되고 있다. 인터넷 기능은 단순 음성 통신뿐만 아니라 매우 다양한 형태의 서비스를 제공할 수 있고 인터넷 감청 표준 기술을 정의할 때 이런 특징들이 고려되어야 한다.

본 고는 인터넷에서 표준화되고 있는 감청 기술에 대한 내용으로 인터넷 감청의 개요와 인터넷 서비스별 감청, 인터넷 응용 서비스에서 감청, 인터넷을 이용한 감청 정보의 전달 기술을 설명한다.

II. 인터넷 감청 개요

인터넷에서 감청 기능의 참조모델은 (그림 1)과 같다[1]. 외형적으로는 일반 감청 참조모델과 비슷하나 패킷통신 기반인 인터넷에서는 통신사업자 영역 부분에서 감청을 위해 기본 모델을 더 세분화하였다.

인터넷 서비스 감청 구조는 크게 수사기관 영역과 통신사업자 영역으로 나누어진다. 수사기관과 통신사업자간에는 세 가지의 핸드오버 인터페이스(Handover Interface: HI)가 존재한다. 핸드오버 인터페이스 1(HI1)은 수사기관에서 통신사업자에게 감청 정보를 요청할 때 사용하는 인터페이스이고 핸드오버 인터페이스 2(HI2)와 핸드오버 인터페이스 3(HI3)은 통신사업자에서 수사기관으로 감청 정보와 감청 내용을 제공할 때 사용하는 인터페이스이다.



HI: Handover Interface
NI: Internal Interception Interface

IRI: : Interception Related Information
CC: : Communication Contents

CCTI: : CC Trigger Interface
CCCI: : CC Control Interface

(그림 1) 인터넷 감청 기능의 참조모델

수사기관은 감청을 요청할 때 감청대상자의 정보 및 감청 처리 방법 등을 상세히 기술하여 HI1 인터페이스를 통하여 통신사업자에게 전달한다. 통신사업자의 감청 운영기능(LI Administration Function: AF)은 수사기관에서 요청한 감청을 이행하기 위해 망 내부에서 사용하는 인터페이스가 있는데 이는 INI(Internal Interface)이다. 그래서 감청 모델에서는 두 종류의 인터페이스가 존재하는데 HI 는 수사기관과 통산사업자간의 인터페이스이고 이는 표준화 대상에 속하고 INI 는 통신 사업자 망 안에서 사용되는 인터페이스로 망사업자 내에서 개별적으로 정의할 수 있다.

1. 감청 정보

감청 표준에서는 HI 에 대한 표준 정의가 가장 중요하다. HI1(Handover Interface 1)은 수사기관에서 통신사업자 망으로 제공하는 인터페이스이다. HI1 에 포함되는 내용은 감청 식별 번호, 감청할 전화번호, 감청 시작과 종료시점, 필요한 정보, HI2 의 내용을 보낼 수사기관측 장비 주소, HI3 의 내용을 보낼 수사기관측 장비 주소, 기타 다른 필요한 정보 등으로 감청 기능을 수행하기 위해 필요한 최소한의 정보가 포함되어야 한다.

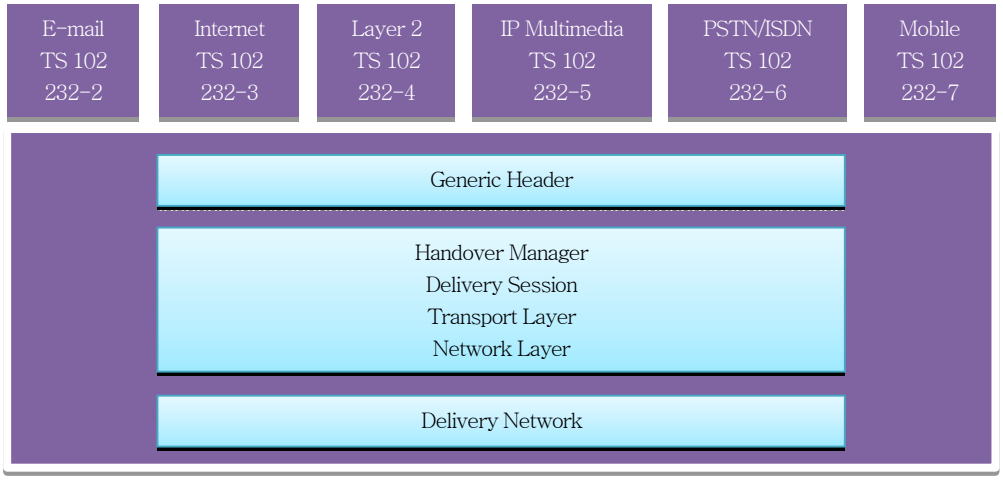
수사기관은 통신사업자에게 HI1 을 공문 형태 요청할 수 있고 전산으로 망을 통하여 요청할 수 있는데 이는 국가에서 정의하는 법에 따라 정의하는 내용으로 일반 감청 표준에서는 다룰 수 없다. 다만, 수사기관에서는 통신망을 직접 제어할 수 없도록 보호하는 기능이 있어야 하며 통신사업자에서는 감청 기능을 남용할 수 없도록 보호 기능이 필요하다. 이런 보호기능에 대한 정의는 국가마다 다르고 각 국가에서 이와 관련한 정의를 개별적으로 해야 한다.

HI2(Handover Interface 2)는 통신사업자 망에서 수사기관으로 전달되는 감청관련 정보(Intercept Related Information: IRI)를 전달하는 인터페이스이다. IRI 는 실제 감청 내용이 아니라 감청 정보, 즉, 감청 종류, 감청 성격, 통화 기간, 감청대상자 위치, 감청 종료 사유, 서버의 주소, QoS 등 통신 내용을 상세히 설명하는 다양한 정보이다. IRI 정보는 ASN.1 과 BER(Basic Encoding Rules)을 이용하여 인코딩되어 통신사업자 망에서 수사기관으로 전달된다.

HI3(Handover Interface 3)는 통신사업자 망에서 수사기관으로 전달되는 감청 내용(Content of the Communication: CC)이다. 이는 전화통화의 경우 실질적인 전화통화 내용이고 이메일의 경우 이메일 내용이다. HI3 의 형태는 감청되는 서비스에 따라 다르게 표현된다. HI2 와 HI3 가 논리적으로 다른 인터페이스를 이용하여 분리가 가능하나 인터넷의 경우 동일한 인터페이스를 사용해도 무방하다. HI2 와 HI3 를 논리적으로 분리한 이유는 아날로그 서킷 스위치 망에서는 HI2 와 HI3 는 동일한 인터페이스를 사용할 수 없어서 분리할 수 밖에 없었고 그 기본적인 틀을 유지하기 위해서 인터넷 감청에서도 분리하였다.

2. ETSI 인터넷 감청 표준 구성

ETSI 의 인터넷 감청 표준 문서는 (그림 2)와 같다[2]. ETSI TS 102 232-1 표준은 IP 전달에 대한 표준을 정의하고 있어 특정 인터넷 서비스와 무관한 범용 인터넷 핸드오버 인터페이스를 정의한다. 그래서 ETSI TS 102 232-2 표준에서 ETSI TS 102 232-7 표준의 모체 표준이 된다. ETSI TS 102 232-1 표준에서는 인터넷 데이터 핸드오버 구조 정의와 HI2 와 HI3 에 추가될 범용 헤더 정보 및 감청 정보 핸드오버를 위한 전달 프로토콜을 정의한다.



(그림 2) ETSI 인터넷 감청 표준 문서의 구성

ETSI TS 102 232-2 표준에서 ETSI TS 102 232-7 표준들은 ETSI TS 102 232-1 에서 정의될 수 없는 해당 서비스 특유의 감청 정보 등을 정의하여 실질적으로 ETSI TS 102 232-2 표준에서 ETSI TS 102 232-7 에서 정의된 감청 기능을 개발할 때 ETSI TS 102 232-1 표준을 함께 참조해야 한다.

나머지 ETSI 인터넷 감청 표준 문서에서 정의되는 내용은 다음과 같다.

- ETSI TS 102 232-2 표준: E-mail 서비스에 대한 감청 표준
- ETSI TS 102 232-3 표준: 인터넷 접속 서비스에 대한 감청 표준
- ETSI TS 102 232-4 표준: Layer 2 서비스에 대한 감청 표준
- ETSI TS 102 232-5 표준: VoIP 서비스에 대한 감청 표준
- ETSI TS 102 232-6 표준: PSTN/ISDN 서비스에 대한 감청 표준
- ETSI TS 102 232-7 표준: 이동통신 서비스에 대한 감청 표준

III. 인터넷 서비스 감청

1. IP 전달 표준(ETSI TS 102 232-1)

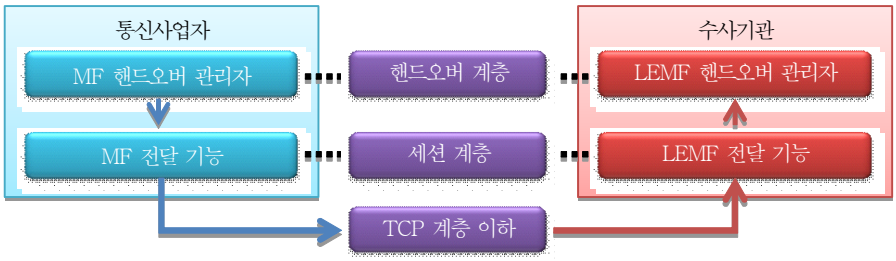
본 표준은 모든 인터넷 감청 표준의 모체 표준으로 인터넷 서비스에서 감청에 대한 전반적인 내용을 정리하고 있다. 인터넷에서 감청하는 방법은 두 가지가 있다. 첫 번째는 네트워크에서 전달되고 있는 Raw IP 패킷을 복사하는 감청 방법으로 '네트워크 수준 감청'이고 이는 네트워크 사업자나 인터넷 접속 서비스 사업자에서 이용하는 방식이다. 두 번째는 VoIP 등과 같이 인터넷을 이용하는 애플리케이션 혹은 프로토콜을 분석하여 감청 정보와 내용을 추출하는 감청 방법으로 '애플리케이션 수준 감청'이고 이는 인터넷 서비스 제공자에서 이용하는 방식이다.

인터넷에서 IRI 와 CC 를 수사기관으로 전달할 때 정의되는 표준 헤더가 있다. 헤더 정보의 내용은 <표 1>과 같다.

<표 1> 핸드오버 메시지의 공통 헤더 필드

필드	설명
Lawful Interception IDentifier(LIID)	감청 구분자로 HI1 에서 할당한 고유번호인데 통신사업자는 HI1 에 해당하는 감청 정보가 발생하면 감청 정보 헤더에 LIID 를 항상 첨부하여 보내어 감청 정보와 내용을 구분함; 감청 대상자, 수사번호, 수사기관번호, 감청의뢰일자 등의 번호의 조합으로 이루어짐
Communication Identifier	Network Identifier(NID), Communications Identity Number(CIN) 및 Delivery Country Code(DCC)로 구성되며 NID 는 통신사업자 번호이고 CIN 은 통신 세션을 구분하며 DCC 는 중재장비의 위치를 표시하는 지역번호임
Timestamp	감청 정보가 생성되는 시간으로 Microsecond 시간으로 표현함
Sequence Number	감청 정보의 순서를 나타내는 일련번호이며 0 에서 232 의 값을 가지며 232 가 넘으면 0 에서 다시 시작함
Direction	통신이 일어나는 방향을 표시하며 감청대상자의 송수신 상태를 표시함
Payload type	CC 인지 IRI 인지 구분함

데이터를 전달하기 위해 통신사업자와 수사기관 간의 (그림 3)과 같이 프로토콜 스택을 구성하여 감청 정보를 처리한다[2].



(그림 3) 감청 프로토콜 스택

핸드오버 계층에서는 한 개 이상의 전달기능을 생성관리하며 오류보고, PDU 결합, 헤더 정보 생성 및 생성된 PDU 를 해당 전달기능에 전달하는 기능을 수행한다. 세션 계층에서는 수사기관과 통신사업자 간의 한 개 이상의 전송 연결을 유지하며 지속적인 Keep-alive 메시지 교환, PDU 암호화/복고화, 데이터 전달 무결성 유지 및 데이터 버퍼링 등의 기능을 수행한다. TCP 이하 계층에서는 수사기관과의 IP 연결을 생성 관리한다.

수사기관과 안전하게 감청 정보를 전달하기 위해 단순 인터넷 연결을 이용하기에는 문제가 많다. 그래서 이용되는 데이터 전달망에 대한 표준 정의가 중요하다. 감청 전달망으로는 사설망을 이용하는 것이 가장 안전하며 전형적인 사설망은 Leased line 이 되겠다. 그 이외에 X.25 와 같이 통신사업자 망에서 강력한 제어 기능이 있는 네트워크를 사용하는 방법이 있고 보안면에서 가장 취약한 퍼블릭 인터넷을 사용하는 방법이 있다.

만약 안전한 전용망을 이용할 수 없으면 기밀성, 신뢰성 및 무결성을 보장하는 강력한 보안 기능을 활용해야 한다. VPN 을 활용하여 종단간, 네트워크간 보안을 제공할 수 있다. ETSI TS 102 232-1 표준에서는 기밀성과 신뢰성을 보장하기 위해 TLS 세션 설정을 권장하며 정보 암호화는 TLS_RSA_WITH_RC4_128_SHA 혹은 TLS_RSA_WITH_AES_256_CBC_SHA 을 이용할 것을 권장한다.

2. 인터넷 접속 서비스(ETSI TS 102 232-3)[4]

인터넷 접속 서비스는 전화, 케이블, 무선 액세스를 통하여 이용자에게 인터넷 서비스를 제공한다. 이용자는 인터넷 접속하는데 있어서 인터넷 서비스 제공자로부터 RADIUS 등과 같은 프로토콜을 이용하여 인증과정을 거친 후에 DHCP, IP Address Pool 등으로 인터넷에 사용 가능한 IP 주소를 할당 받게 되는데 이런 일련의 과정을 활용하면 인터넷 접속 감청이 가능하다. 인터넷 감청측면에서는 감청대상자가 DHCP 를 통하여 IP 주소를 할당 받는 사실이 중요하며 그 순간부터 감청이 시작된다. 감청대상자가 사용한 IP 주소를 반납하게 되면 바로 다른 이용자에게 그 주소가 할당될 수 있으므로 그 순간부터 감청이 중단되어야 한다.

인터넷 접속 감청에서는 감청대상자의 아이덴티티(Identity)가 매우 중요하며 아이덴티티는 Username, NAI(Network Access Identifier), IP 주소, MAC 주소 혹은 감청대상자를 식별할 수 있는 unique ID 가 될 수 있다.

인터넷 접속 서비스에서의 주요 감청 정보는 네트워크 접속 시도 시점, 네트워크 접속 수락 혹은 거절 시점, 상태변화 및 접속 지점 등이 될 수 있다. 감청 내용은 감청대상자의 주소가 포함된 모든 IP datagram 이 된다. 인터넷에서는 IP 주소 스푸핑이 가능하기 때문에 수사기관은

감청대상자의 주소가 포함된 모든 IP datagram 이 감청대상자가 직접 보낸 패킷이 아닐 수 있음을 인지해야 한다.

3. Layer 2 서비스(ETSI TS 102 232-4)[5]

ETSI TS 102-232-4 는 감청대상자에 대해 정해진 IP 주소는 없고 Layer 2(MAC 등) 주소나 종단 인터페이스 정보를 이용한 감청에 대한 표준이다. 즉, 감청대상자가 접속한 인터페이스 즉, 액세스 네트워크에서 감청하는 방법이 된다. 액세스 네트워크는 종단 이용자에게 인터넷 접속을 할 수 있도록 가능하게 해준다. 대표적인 액세스 네트워크는 DSL, 전화, 케이블, 무선 네트워크 등이다.

Layer 2 서비스에서 감청하기 위해 감청대상자를 구분할 수 있는 구분자가 필요하며 구분자는 접속에 사용되는 장비나 네트워크를 접속하는 접속 방법에 따라 다르게 표현된다. 가장 보편적으로 사용할 수 있는 구분자는 MAC 주소 혹은 xMAC 주소로 감청대상자가 사용하는 장비를 구분할 수 있다. 감청대상자가 사용하는 장비의 MAC 주소로 구분이 불가능하면 xDSL-line 의 종단점 ID, Cable-line 종단점 ID 혹은 E.164 번호 등으로 구분이 가능하다.

Layer 2 서비스에서 사용될 수 있는 감청 이벤트는 이용자 인증이 이루어지는 로그온 상태, 데이터를 전달하는 데이터 전송 상태, PPP 세션 종료로 로그오프 상태, 그리고 링크 오류로 인한 연결 손실 상태 등이 될 수 있어 이런 상태 정보로 감청 정보(IRI)를 구축할 수 있다. Layer 2 에서 감청은 패킷 캡처링 형태로 가능하며 감청 내용(CC)은 감청된 감청대상자가 Layer2 접속을 통하여 Layer 2 데이터를 송수신하는데 전달되는 데이터 패킷들이다.

IV. IP 응용 서비스 감청

1. E-mail 서비스(ETSI TS 102 232-2)[3]

E-mail 은 수사기관에게는 매우 중요한 감청 응용이다. E-mail 감청은 감청대상자의 메일박스 내용만 감청 대상이 되는 것이 아니라 이메일 서비스의 과정도 매우 중요한 감청 대상이다. 그래서 E-mail 감청 과정은 메일 송신 감청, 메일 수신 감청 그리고 메일 다운로드 감청 등으로 분류될 수 있다.

감청대상자가 이메일을 전송할 때 감청대상자가 사용하고 있는 이메일 클라이언트와 이메일 수신자의 메일박스가 존재하고 있는 이메일 서버 간의 통신으로 이루어진다. 이때, 이메일 송신

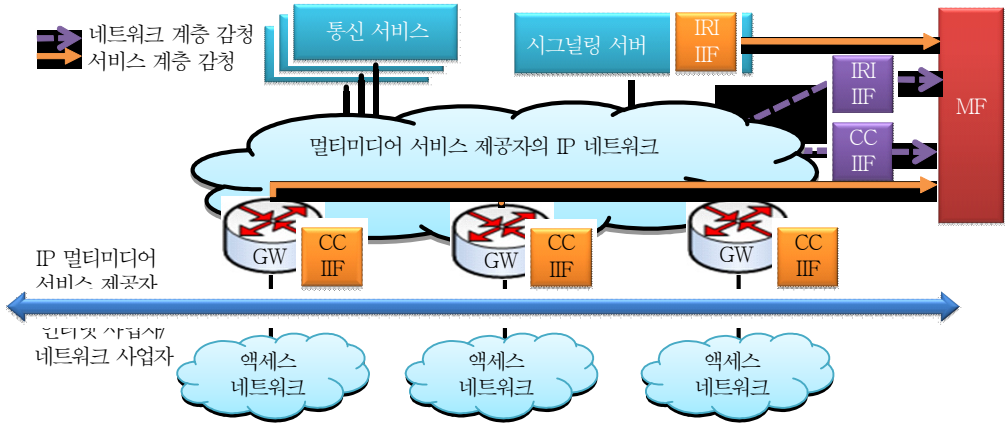
이벤트만 감청되고 실질적으로 상대방의 메일박스로 이메일 송신 실패/성공여부는 감청대상이 되지 않는다. 그 이유는 수신자의 이메일 박스에서 성공/실패의 확인 메시지를 보내지 않는 경우가 많기 때문이다. 감청 내용은 감청대상자가 보낸 E-mail envelop, text 등이 되고 감청 정보는 국가의 법에서 규정된 내용에 따라 상이할 수 있지만 이메일 서버와 클라이언트의 주소정보, 사용 프로토콜, 이메일 송신자, 수신자, 이메일 ID, 상태, AAA 정보 등이 된다.

감청대상자가 이메일을 수신할 때 이메일 송신자의 이메일 클라이언트와 감청대상자의 메일박스가 존재하고 있는 이메일 서버 간의 통신으로 이루어진다. 이때, 감청대상자의 이메일 수신 이벤트만 감청된다. 감청 내용은 감청대상자가 수신한 E-mail envelop, text 등이 되고 감청 정보는 이메일 서버와 클라이언트의 주소정보, 사용 프로토콜, 이메일 송신자, 수신자, 이메일 ID, 상태 등이 된다.

감청대상자가 자신의 메일을 확인할 때 메일박스에서 이메일을 다운로드하게 되는데 이런 과정에서 감청대상자의 이메일 클라이언트와 이메일 서버 간의 통신이 이루어져 별도의 이메일 이벤트로 볼 수 있다. 그래서 감청대상자가 수신한 이메일과 감청대상자가 확인하는 이메일에는 차이가 있다. 감청 내용은 감청대상자가 읽게 되는 E-mail envelop, text 등이 되고 감청 정보는 감청대상자의 이메일 서버와 클라이언트의 주소정보, 사용 프로토콜, 이메일 송신자, 수신자, 이메일 ID, 상태, AAA 정보 등이 된다.

2. IP Multimedia 서비스(ETSI TS 102 232-5)[6]

IP 멀티미디어 서비스는 시그널링 서버 기능으로 이용자들을 연결하여 통신이 가능하게 하는 서비스로 SIP 나 H.323 을 이용하는 VoIP 서비스와 메신저, 다자간 통신 등이 된다. (그림 4)



(그림 4) IP 멀티미디어 서비스 감청 모델

에서는 IP 멀티미디어 서비스 감청 모델을 보여주고 있다. 다양한 IP 멀티미디어 서비스는 시그널링 서버를 통하여 제공되고 있으며 이용자는 다양한 액세스 네트워크를 접속하여 액세스 네트워크와 IP 멀티미디어 서비스 네트워크와의 상호작용으로 IP 멀티미디어 서비스를 받고 있다. 그래서 네트워크 사업자와 서비스 제공자 사이의 기능적인 분리가 이루어진다.

IP 멀티미디어 서비스 감청에 있어서 두 가지 방법이 있다. 첫 번째는 네트워크 계층 감청으로 멀티미디어 서비스 제공자의 네트워크에 있는 스위치 등과 같은 네트워크 장비에서 지나가는 패킷을 캡처하여 감청하는 방법이다. 이때, 실질적인 감청에 필요한 패킷인지를 분석하는 기능과 및 필요한 패킷만 추출하는 필터링하는 기능이 필요하며 필터링된 패킷으로 감청 정보와 감청 내용에 대한 분류 기능이 필요하다.

다른 방법은 서비스 계층 감청으로 시그널링 서버와 게이트웨이에서 감청 기능이 포함되어 있는 상태에서의 감청하는 방법이다. 시그널링 서버는 이용자들에게 착신지에 대한 정보를 제공하기 때문에 시그널링 서버를 통하여 감청대상자의 통신이 시작되는지 알 수 있어서 IRI 감청이 가능하고 실질적인 통신 내용은 IP 멀티미디어 게이트웨이를 통하여 이루어져서 CC 에 대한 감청이 이루어진다.

IP 멀티미디어 서비스에서 감청대상자에 대한 구분이 필요한데 SIP 프로토콜에서는 TEL URI, SIP URI, E.164 번호 등으로 이용할 수 있고 H.323 에서는 H.323 URI, H.323 ID 및 E.164 번호가 이용이 된다.

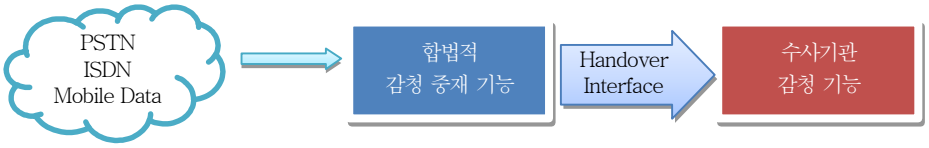
IP 멀티미디어 서비스 호에 대한 구분은 CIN(Communication Identity Number)으로 구분할 수 있는데 SIP 프로토콜에서는 CIN 을 SIP 메시지의 SDP 부분에서 'O' 필드의 값으로 이용이 가능하고 H.323 프로토콜에서는 CIN 을 H.225.0 Call ID 를 이용하면 된다.

IP 멀티미디어 서비스에서의 감청이 발생되는 시점은 감청대상자가 통신을 시도되는 시점, 통신을 성공한 시점, 통신이 실패 시점, 통신상태 변경 시점, 서비스나 서비스 파라미터 변경 시점 그리고 통신 위치 변경 시점 등으로 구분된다. 감청 정보는 통신이 시도된 상대방(상대방에 대한 정보), 사용된 서비스와 파라미터, 상태 정보 그리고 타임스탬프가 된다. 다자간 통신에서도 같은 방법으로 감청이 된다.

감청 내용은 서비스 사업자 망에 전달되는 모든 RTP 및 RTCP 패킷으로 IP 헤더 이상의 패킷을 전달하며 전달할 때 감청관련 CID 가 포함된 세션 정보와 함께 전달되어 수사기관에서 통신 내용이 어떤 IP 멀티미디어 호에 대한 감청 내용인지 알 수 있도록 관련 정보와 함께 수사기관으로 전달되어야 한다.

V. 인터넷을 통한 감청 정보 전달

인터넷 감청 표준 중에서 인터넷을 이용하여 PSTN, ISDN, 이동통신망 서비스에 대한 감청 정보와 감청 내용을 전달하는 표준, 즉 ETSI TS 102 232-6 표준[7] 및 ETSI TS 102 232-7[8] 표준이 정의된다. 각 표준은 PSTN/ISDN 서비스 및 이동통신 서비스에 대한 감청 표준을 정의한다.



(그림 5) 인터넷을 통한 감청정보 전달

PSTN, ISDN 에서 발생되는 감청 정보는 TS 101 671 “Lawful Interception; Handover interface for the lawful interception of telecommunications traffic” 표준을 따른다. TS 101 671 표준은 모든 감청 표준의 모체 표준이며 PSTN/ISDN 에서 감청 표준으로 사용된다. PSTN, ISDN 의 감청 내용은 RTP 프레임으로 변환되어 수사기관으로 전달된다. RTP 프레임으로 변환될 때 수사기관이 RTP 프레임을 해독할 수 있도록 키와 같은 관련 정보를 제공해야 하는데 그런 정보를 부가 정보라고 한다. 부가 정보는 미디어 포맷, 해독 키, 세션 정보 등이 된다.

이동통신망에서 발생되는 감청 정보는 ETSI TS 133 108: “Universal Mobile Telecommunications System(UMTS); 3G security; Handover interface for Lawful Interception(3GPP TS 33.108)” 표준을 따른다. TS 102 232-7 문서는 3GPP TS 33.108 표준에서 정의한 감청 표준을 그대로 수용하면서 정의된 감청 정보를 TS 102 232-1 에서 정의한 감청 정보로 맵핑시켜주고 있다.

VI. 결 론

ETSI 에서는 인터넷에서 합법적인 감청 구조와 감청 기능 요소와 관련하여 표준을 정의하고 있으며 현재까지 인터넷과 관련하여 7 개의 감청 표준으로 정의하고 있다. 본 고는 ETSI 에서 정의한 인터넷 감청 표준들의 문서를 정리 및 요약하였다. ETSI TC LI 에서는 이런 감청 표준을 지속적으로 개발을 진행하고 있다. 본 고를 통하여 ETSI 에서 정의한 인터넷 감청 표준을 이해하고 인터넷에서 감청하는 방법에 대해서 파악한다.

국내에서는 통신비밀보호법을 통하여 통신 서비스에 대한 합법적 감청을 수행하고 있으나 현재 통신비밀보호법으로는 ETSI 표준에서 정의하는 그런 수준의 감청 협조를 요구하기는 어렵다. 현재 전기통신사업자에게 감청 수행을 위한 감청 설비 구비를 의무화하는 내용이 포함된 통신비밀보호법 일부 개정안이 발의된 상태에 있다. 법률 개정에 앞서 감청하는 방법에 대해서 정의해야 하고 또한 감청 기술과 관련하여 감청 표준 및 감청 기술 개발이 매우 중요하다.

<참 고 문 헌>

[1] ETSI Report, “Lawful Interception (LI) Interception domain Architecture for IP networks”, ETSI TR 102 528, Version 1.1.1, Oct. 2006.

[2] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 1: Handover specification for IP delivery”, ETSI TS 102 232-1, Version 2.4.1, July 2008.

[3] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 2: Service-specific details for E-mail services”, ETSI TS 102 232-2, Version 2.3.1, Nov 2007.

[4] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 3: Service-specific details for internet access services”, ETSI TS 102 232-3, Version 2.1.1, Dec 2006.

[5] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services”, ETSI TS 102 232-4, Version 2.1.1, Dec 2006.

[6] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services”, ETSI TS 102 232-5, Version 2.3.1, April 2008.

[7] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services”, ETSI TS 102 232-6, Version 2.3.1, August 2008.

[8] ETSI Standards, “Handover Interface and Service-Specific Details(SSD) for IP delivery; Part 7: Service-specific details for Mobile services”, ETSI TS 102 232-7, Version 2.1.1, March 2008.

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.