Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.701

IPTV 방송서비스에서의 개인정보보호에 관한 연구*

이 진 혁,† 김 승 주‡
고려대학교 정보보호대학원

Study on Privacy in the IPTV Broadcasting Service*

Jinhyuk Lee,† Seungjoo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

세계적으로 IPTV를 중심으로 디지털 케이블 TV(이하 DCATV)를 포함한 디지털 유료방송 서비스의 이용자 수가 증가하고 있고, 다양한 서비스가 제공되고 있다. 제공되는 서비스 중 주문형 비디오(이하 VOD), 홈쇼핑과 같은 결제 콘텐츠, 시청 이력, 선호 채널 분석을 통한 사용자 맞춤형 콘텐츠에서는 사용자의 개인정보를 필요로 한다. 사용자의 개인정보는 방송사업자에서 제공되는 셋톱박스(이하 STB)를 통해 방송사업자에게 전송되는데, 방대한 양의 사용자 개인정보가 축적되기 때문에, 유출 시 사생활 침해나 재산 피해와 같은 사회적 혼란을 야기할 수 있다. 본 논문은 방송사업자가 서비스 제공을 위해 개인정보의 수집에 관한 동의를 얻는 과정에서 개인정보의 수집 및 사용에 대한 동의가 제대로 이루어지고 있는지, 개인정보를 적절하게 수집하고 있는지에 대한 실태를 분석하고 실제 전송되는 네트워크를 분석하여, IPTV 환경에서의 개인정보보호에 대한 문제점을 제시하고 그에 대한 해결방안을 제시한다.

ABSTRACT

The number of subscriber of digital pay TV service such as Digital Cable TV and IPTV is increasing from various kind of service provider world widely. These services require personal information of users to provide VOD(Video on Demand) and customized contents. Therefore, massive amount of personal information collected by service provider can cause social confusion such as leakage of privacy and property damage. This paper investigates whether broadcasting stations are providing enough notification for privacy policy and methodology of collecting private information in proper way. Furthermore, we analyze actual network traffic of IPTV service between user and service provider to suggest solution of privacy protection along with current status analysis.

Keywords: Digital Pay-TV, IPTV, Privacy

I. 서 론

IPTV(Internet Protocol Television)와 DCATV(Digital cable television)는 지상파를 포함한 다채널 실시간 방송 콘텐츠와 VOD(Video on Demand) 콘텐츠를 제공하는 디지털 양방향 TV 서비스이다. IPTV는 초고속 인터넷망을 통해 서비스를 제공하며, DCATV는 지역 방송에서 제공하는 광케이블과 동축케이블이 결합된 광동축 혼합망(HFC : Hybrid Fiber Coaxial)을 통해 서비스를 제공한다. 전송방식은 다르지만 TV를 통해 고화질의 HD(High definition) 방송을 볼 수 있다는 점과 VOD, 게임, 홈쇼핑과 같이 방송과 통신이 융

Received(12. 01. 2015), Modified(1st: 04. 22. 2016, 2nd: 05. 26. 2016), Accepted(06. 07. 2016)
* 본 논문은 2015년도 하계 학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2016년 고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었습니다.
† 주저자, leejinhyuk@korea.ac.kr
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

합된 양방향 부가서비스를 제공한다는 점에서 비슷한 산업 구조를 가진다. Table 1.은 2015년 2월 기준 IPTV와 DCATV의 가입자 현황이다[1]. 2015년 2월 기준 IPTV의 가입자 수는 1,096만, DCATV의 가입자 수는 721만에 달하고 있으며, 앞으로도 지속적으로 증가할 전망이다.

디지털 양방향 TV 서비스는 그동안 TV를 통해서 일방적으로 전달되던 정보의 흐름을 사용자가 원하는 정보를 찾아볼 수 있도록 허용한다. 채널을 통해 프로그램과 이와 관련된 정보뿐만 아니라 여행, 기상, 게임, 증권 정보와 같은 방송서비스와 독립적인 정보를 사용자에게 제공하고, 사용자는 TV시청 중 자신이 원하는 정보를 불러와 이용할 수 있다. 또한, 그동안 인터넷상에서 이루어지던 전자상거래가 TV를 통해서도 이루어질 수 있어 T-commerce라는 TV를 통한 전자상거래의 도래를 가져왔다[2]. 이러한 양방향 데이터 통신은 방송사업자에서 제공하는 STB(Set-Top Box)를 통해 이루어지며, 사용자 ID, 서비스 이용 기록, 결제 정보와 같은 개인정보가 STB를 통해 방송사업자로 전송된다. 방송사업자에서는 STB를 통해 전송 받은 개인정보를 수집하여 축적하게 되는데, 사용자의 개인정보를 수집하기 위해서는 사용자의 동의가 우선 되어야 하며, 적법한 절차에 의해 동의가 이루어져야 한다. 2013년 11월 LG전자는 스마트TV를 통해 사용자의 동의 없이 시청 채널 및 시간, 미디어 파일 이용 목록과 같은 사용자의 개인정보를 무단으로 수집해 맞춤광고에 활용해온 것으로 논란이 되었다[3].

Table 1. Number of Digital Pay-TV subscribers

DCATV/IPTV	Service Provider	Subscriber
DCATV	A사	2.5 mil
	B사	1.59 mil
	C사	1.58 mil
	D사	0.18 mil
	E사	0.69 mil
	F사	0.67 mil
DCATV Total		7.21 mil
IPTV	G사	5.99 mil
	H사	2.97 mil
	I사	2 mil
IPTV Total		10.96 mil
Total		20.11 mil

(mil:million)

본 논문에서는 국내에서 200만명의 가입자를 보유하고, STB 제품 측면에서는 전세계에서 높은 점유율을 차지하는 Android 기반의 특정 STB를 사용하는 국내 I사의 IPTV 서비스를 대상으로 사용자의 개인정보 수집을 동의하는 과정에서 발생하는 문제점을 제시하고, 실제 방송서비스에서 STB를 통해 방송사업자로 전송되는 사용자의 개인정보 데이터를 수집하고 분석한다. 분석한 결과를 기반으로 IPTV가 해결해야 하는 디지털 양방향 방송 환경에서의 개인정보 수집의 문제점과 개인정보 보호방안을 제시한다.

II. 관련 연구

2.1 IPTV 산업구조

IPTV 산업구조의 구성도는 Fig. 1.과 같다[4]. IPTV 사업자는 크게 PP/CP, SP, NP로 분류할 수 있다. PP(Program Provider)/CP(Content Provider)는 방송 채널 사용 사업자로 방송 프로그램과 콘텐츠를 제작, 구매하여 SP를 통해서 송출하는 사업자이며, 대표적인 예로 Mnet, YTN, OCN과 같은 케이블 방송사가 있다. SP(Service Provider)는 IPTV 방송 사업자로 SK 브로드밴드, KT, LG 유플러스와 같은 IPTV 방송 사업자가 있다. NP(Network Provider)는 전송망 사업자로, 인터넷 서비스 사업자를 말한다. 요즘은 대부분의 SP가 자체 전송망을 구축하는 추세이므로 SP와 NP가 결합된 구조를 가진다. PP/CP가 프로그램을 생산하는 주체라면 SP는 PP/CP로부터 프로그램을 받아 사용자에게 전달하는 역할을 한다.

사용자는 IPTV 서비스를 사용하는 과정에서 STB를 통해 방송사업자와 통신을 하게 된다. IPTV는 STB와 사업자 서버간의 통신이 인터넷망을 통해 이루어지는 반면, DCATV는 동일한 구조에서 STB

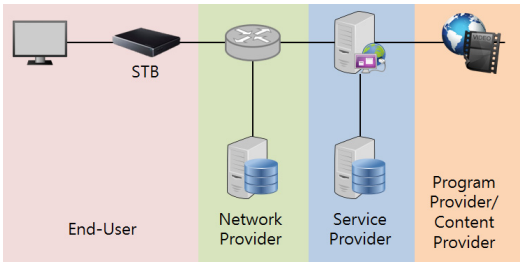

Fig. 1. Digital Pay-TV industry structure

와 사업자 서버와의 통신이 동축케이블을 통해 이루어진다는 차이가 있으나 전체적인 시스템의 구조는 동일하다. 사용자는 STB를 통해 TV프로그램 시청은 물론 SP가 제공하는 VOD, 게임, 홈쇼핑과 같은 다양한 콘텐츠를 이용하는 구조이다. 서비스를 이용하는 과정에서 STB를 통해 서비스 이용정보, 결제정보와 같은 사용자의 개인정보가 방송사업자에게 전달되고, 방송사업자는 사용자 개인정보를 저장하고 분석하여 개인맞춤형 서비스와 같은 부가 서비스를 제공하는데 활용하게 된다.

2.2 STB 통신 프로토콜

STB에서 IPTV 서비스의 기능을 제공하기 위해 많은 통신 프로토콜이 사용된다. 다양한 어플리케이션과 IPTV 서비스 기능을 지원하기 위해 각기 다른 프로토콜을 이용해 데이터통신이 이루어진다. ITU에서는 IPTV 관련 통신 프로토콜을 다음 Table 2.와 같이, TCP/IP 계층에 의해 분류하였다[5].

본 논문에서 분석한 IPTV의 통신에서 수행된 주요 프로토콜은 다음과 같다.

- HTTP(Hypertext Transfer Protocol)
  방송사업자의 네트워크에 위치한 미들웨어 서버와 사용자의 STB 간의 커뮤니케이션을 위한 통신
- RTSP(Real-Time Streaming Protocol)
  재생, 일시 정지, 빨리 감기와 같은 미디어 세션의 행동을 제어하기 위한 통신
- RTP(Real-time Transport Protocol)
  실시간 미디어 콘텐츠의 전송 (오디오, 비디오)하기 위한 통신
- IGMP(Internet Group Management Protocol)
  사용자 STB의 TV 채널 변경을 위한 통신

Table 2. IPTV Protocols

Layer	Protocols
Application Layer	DHCP, DNS, DVB-IPTV, FEC, FLUTE, FTP, HTTP, IPDC CDP, LC, MBMS, RTP, RTSP, SIP, SNTP, TLS
Transport Layer	TCP, UDP
Network Layer	BGMP, ICMP, IGMP, IP, MLD, MSDP, PIM-SM, Anycast-RP, SSM

2.3 IPTV 서비스

IPTV는 수많은 새로운 서비스들을 가능하게 하였다. ITU에서는 IPTV의 서비스를 콘텐츠 서비스, 양방향 서비스, 통신 서비스로 분류하였으며[6], 각 분류에 해당하는 서비스를 정리하면 다음 Table 3.과 같다.

Table 3. IPTV Service List

Category	Services
Content Services	Linear TV (audio, video and data)
	Linear Broadcast Audio
	Linear TV with Trick Modes
	Multi-View service
	Pay Per View (PPV)
	Personal Broadcast Service
	PVR service (network or client-based)
	Time-shift TV
	Video on Demand (VoD)
	Near Video on Demand
	Content Push
	Music on Demand (MoD)
	Content download service
	Service Information (EPG, ECG)
	3rd party content services
	End-user Originated content
	Regulatory Information services
	Advertising
	Hybrid services
Interactive Service	Interactive TV (iTV)
	Learning services (education, languages, …)
	Information services (news, weather, traffic, …)
	Entertainment services (photo, games, karaoke, blog)
	Portal services
	Commerce services (security, banking, shopping, …)
	Interactive Advertising
Communication Service	Communication services (e-mail, IM, SMS, Chat, …)
	Communications Messaging
	Presence services

III. IPTV 방송서비스에서 수집되는 개인정보

3.1 서비스 가입신청서 분석

본 절에서는 사용자가 IPTV 서비스를 이용하기 위해 작성해야 하는 가입신청서에서의 개인정보 수집 항목을 분석하고, 문제점을 도출한다.

3.1.1 개인정보 수집 동의 항목

IPTV 서비스를 이용하기 위해 사용자가 직접 작성해야 하는 가입신청서에는 개인정보 수집과 관련된 필수 동의 항목이 있다. 개인정보 수집은 필수 동의 항목에 포함되기 때문에, 사용자가 동의를 하지 않으면 해당 서비스를 이용할 수 없다. 방송사업자별로 가입신청서의 양식은 다르지만, 수집하는 개인정보 항목은 동일하다. 본 논문에서는 분석한 국내 IPTV 사업자들의 IPTV 서비스 가입신청서에서의 개인정보 수집 동의 항목 중 공통 항목들을 표로 정리하면 Table 4.와 같다. 수집하는 개인정보 항목에는 고유식별번호(주민등록번호·여권번호·외국인등록번호)가 포함되어 있으며, 민감정보에 해당하는 가입자의 위치정보, 신용정보, 과금정보도 별도의 동의 절차 없이 일괄동의 항목에 포함되어 있다. 또한 품질정보, 이용내역, 가입정보, 쿠키, 접속로그, 접속IP와 같은 서비스의 전반적인 이용정보를 모두 포함한 채, 필수 동의 항목과 선택 동의 항목의 구분 없이 일괄 필수 동의 항목으로 사용자의 동의를 받고 있다.

3.1.2 문제점

정보통신망 이용촉진 및 정보보호 등에 관한 법률과 개인정보보호법에 따르면 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 수집하여야 한다[7][8]. 하지만 가입신청서 상에서는 앞 절에서 언급한 모든 항목에 대해 일괄 동의를 받기 때문에 어떤 항목이 어떤 서비스를 이용하기 위해 수집되어야 하는 최소한의 범위인지에 대한 명시가 없으며, 각 항목의 이용 목적에 대한 명시도 없다. 따라서 사용자 입장에서는 개인정보 수집에 대한 동의를 하더라도, 실제로 본인의 개인정보 중 어떤 항목이 어떤 목적으로 이용되는지 알 수가 없다. 그리고 원칙적으로 수집이 금지되어 있고, 정보 주체의 별도의 동의가 있어야 수집이 가능한 주민등록번호, 여권번호, 외국인등록번호와 같은 고유식별정보가 개인정보 수집 항목에 포함된 채 일괄동의가 이루어지고 있다. 또한 개인정보 수집 항목 중 요금 할인을 위해 수집하는 신체 장애 여부와 같은 민감정보는 필수 동의가 아닌 선택 동의 항목으로 분류되어야 하나, 역시 일괄 동의 항목에 포함되어 있다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 개인정보보호법에서 개인

Table 4. Personal information collected on the Service agreed entry form

Collect and use personal information (required agreement)	
1. Collecting information	Subscriber Name, Social Security Number, Passport Number, Immigration Information, Alien Registration Information, Contact, Email Address, Payer Name, Social Security Number, Accounts (Card) Information, Terminal Information, Location Information, Credit Information, Billing Information, Quality Information, Use History, Subscription Information, Cookies, Access Log, Connecting IP, Statistical Data, Configuration Information Website, etc
2. Collection and utilization purposes	Identification, authentication, mobile identity verification services, credit judgment, billing, service, product offerings and descriptions, using the frequency identification and service delivery according to demographic characteristics, personalized service, services, product development and specialization, the user and statistics on services and analysis, Luggage delivery, Customer Relationship Management, and other business transactions, identity theft protection, Wi-Fi location services and broadcast audience measurement and partnership services and guidance, contract enforcement, business consignment, cancellation refunds descriptions, location-based information and advertising transport services
3. Period of Retention and use	After using the service during the subscription period and termination fees for settlement, the dispute holds up to six months, compared to rates paid in full use

Table 5. ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC. and PERSONAL INFORMATION PROTECTION ACT violations in Sign Agreement

Law	Article	Main Content	Problem
ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.	Article 23 (Restrictions on Collection of Personal Information)	No provider of information and communications services may collect personal information of a person, such as ideology, faith, and past medical record, which is anticipated to otherwise intrude seriously upon a right, an interest, or privacy of the person	Collecting Personal information that could violate your privacy
		Every provider of information and communications services shall, whenever it collects personal information of a user, limit the extent of collection of personal information to the minimum information required for providing the information and communications services	No statement for the minimum range required for the service
	Article 23-2 (Restriction on Use of Resident Registration Numbers)	A provider of information and communications services may not collect/use users' resident registration numbers	Including Resident Registration Numbers in the collection of personal information items
PERSONAL INFORMATION PROTECTION ACT	Article 4 (Rights of Subject of Information)	A subject of information has the right to choose and decide whether he/she consents to the management of his/her personal information, the scope of consent.	cannot choose whether he/she consents and cannot decide the scope of consent
	Article 23 (Restrictions on Management of Sensitive Information)	Collecting sensitive information requires a separate agreement.	No separate agreement
	Article 24 (Restrictions on Management of Unique Identifying Information)	Collecting unique identification information requires a separate agreement.	No separate agreement
	Article 24-2 (Restriction on Management of Resident Registration Numbers	Collecting resident registration numbers requires a separate agreement.	No separate agreement
	Article 22 (Methods of Obtaining Consent)	Obtaining Consent of a subject of information requires seperation of the essential information for service and the selective information for additional services.	No seperation of essential information and selective information

정보 수집 관련 조항 내용과 가입동의서에서의 항목을 비교하였을 때 문제가 되는 점을 정리하면 Table 5.와 같다.

이와 같이, 가입신청서 상에서의 개인정보 수집은 형식적인 모양만 갖췄을 뿐, 제대로 이루어지고 있다고 볼 수 없다. 개인정보의 수집과 이용은 개인정보 오남용, 정보의 위험과 같은 역기능에 대해 반드시 고려되어져야 하며, 고유식별정보, 민감정보와 같은 정보는 유출시 피해가 커질 수 있기 때문에 철저한 관리가 되어야 한다.

3.2 STB 네트워크 패킷 분석

본 절에서는 실제 서비스되고 있는 IPTV STB의 네트워크 패킷을 분석함으로써 서비스 이용시 전송되는 사용자의 개인정보 데이터를 식별하고 식별된 데이터에 대해 분석하였다.

3.2.1 실험 환경

실험 대상인 I사의 IPTV STB는 안드로이드 운영체제 기반의 STB이다. STB와 방송사업자 사이에 전송되는 네트워크 데이터를 분석하기 위해, STB와 방송사업자 사이의 인터넷 공유기에 PC를 직접 연결하였다. 공유기의 Port Mirroring[9] 기능을 이용하여 양 구간 사이에 전송되는 네트워크 패킷을 PC로 복제 전송하여 캡쳐하였고, 네트워크 분석 도구 소프트웨어 Wireshark를[10] 통해 캡쳐한 네트워크 패킷의 내용을 분석하였다. 실험환경에 대한 구성도는 Fig. 2.와 같다.

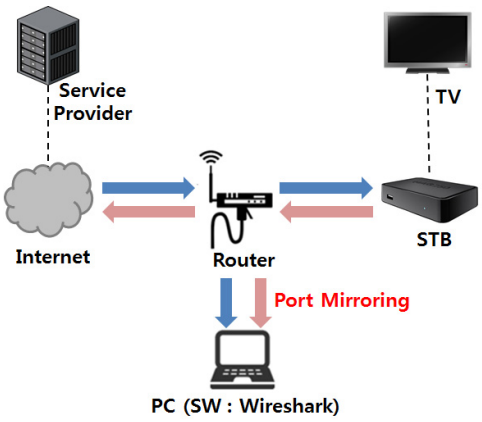

Fig. 2. Network packet analysis environment

3.2.2 분석 방법

IPTV STB의 네트워크 패킷을 분석하기 위해 IPTV 서비스에서 사용자가 가장 많이 사용하는 기능을 Use Case로 정하여, 다음 Table 6.과 같이 구분하였다. 본 실험에서는 각 Use Case에서 발생하는 네트워크 패킷을 캡쳐하고, Wireshark를 통해 패킷의 내용을 분석하여, 전송되는 개인정보를 수집한다.

Table 6. Use Cases by user in IPTV Service

Use Case	Descryption
STB Power On	Power on the STB is connected to the Internet router, capture the network packets to the IPTV service during the initial connection
Changing TV Channel	Capturing network packets in process of changing TV channel
VOD play	Capturing network packets in the process of selecting and reproducing the VOD
Run web application	Capturing network packets while surfing websites after running the web application
STB Power Off	Off the STB's power switch and capture the network packets while the power of the device off

3.2.3 서비스 이용 단계별 패킷 분석

- **STB Power On**

STB의 전원을 키면 먼저 STB의 사용자 인증을 하는데, 사용자의 ID(user number)와 STB 기기의 MAC 주소를 통해 사용자 인증을 한다. 이 과정에서 다음 Fig. 3.과 같이 사용자의 User number, STB 단말 정보, STB 기기의 MAC 주소, STB의 전원을 켠(act) 시간의 정보가 전송된다.

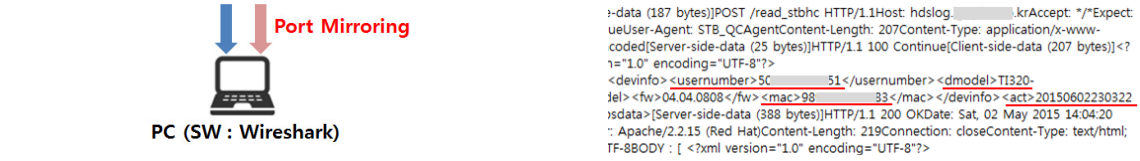

Fig. 3. Network packets when STB boots

사용자 인증 단계를 거치고 나면 IPTV 서버로부터 전체 채널에 대한 리스트와 각 채널에 대한 멀티캐스트 IP 주소 정보가 STB로 전송된다. 이 때, 다음 Fig. 4.와 같이, 각 채널에서 방송중인 현재 프로그램 정보와 각 프로그램의 썸네일 이미지가 있는 URL 주소가 포함된 정보가 전송된다. 전송되는 썸네일 이미지 주소를 통해서는 성인채널을 포함하여 시청 권한이 없는 채널의 썸네일 이미지를 볼 수 있다.

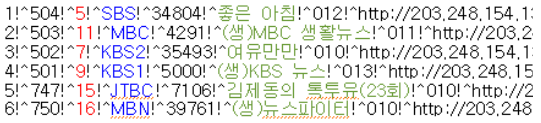

Fig. 4. Channel and program information

- **채널 변경**

STB의 채널 수신 요청은 IGMP 프로토콜을 이용해 통신하며, 사용자가 채널을 변경하면 STB로부터 시청중인 채널에 대한 IGMP Leave 메시지가 전송되고 선택한 채널에 대한 IGMP Join 메시지가 전송된다. 다음 Fig. 5.는 KBS2(멀티캐스트 주소 : 233.18.145.120) 채널을 시청 중에 MBC (멀티캐스트 주소 : 233.18.145.194)로 채널을 변경했을 때의 네트워크 패킷 내용이다. 이와 같이, 사용자가 채널을 변경할 때 사용자가 시청한 채널과 시청한 시간이 STB를 통해 방송사업자로 전송된다.

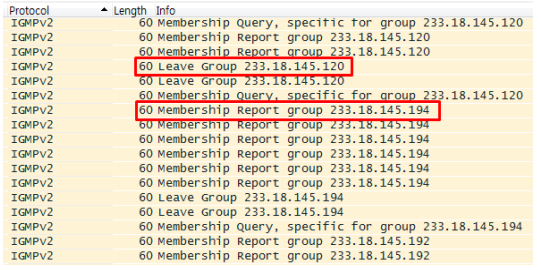

Fig. 5. Network packets when changing channels

- **VOD 재생**

영화 VOD 시청 및 TV 다시보기 콘텐츠를 이용할 때, 시청한 VOD의 제목과 해당 VOD의 썸네일 이미지가 전송된다. 또한 Fig. 6.과 같이, 시청한 VOD와 유사한 장르의 VOD 컨텐츠 목록이 사용자 맞춤형 콘텐츠 제공을 위해 전송되며, 시청 가능 기간이 한정되어 있는 유료방송을 구매해서 시청하였을 때에는 해당 VOD의 사용 만료일 정보가 Fig. 7.과 같이 네트워크 패킷에 포함되어 전송된다.

Fig. 6. VOD title and thumbnail image

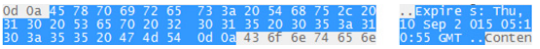

Fig. 7. The expiration date of the VOD Pay-per-view

- **웹 어플리케이션 실행**

STB 내의 웹 어플리케이션을 실행하여 웹 서핑을 하게 되면 Fig. 8.과 같이, 사용자가 어떤 웹사이트에 방문하였는지에 대한 사이트 주소와 방문 시간이 전송된다. 국내 포털 사이트의 경우 로그인을 했을 때 로그인한 ID도 패킷에 남아 있었으며, 비밀번호는 패킷에 검출되지 않은 것으로 보아 암호화 되어 전송되는 것을 유추할 수 있다.

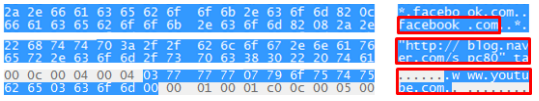

Fig. 8. Web addresses of sites visited

- **STB Power Off**

STB의 전원을 끄면 다음 Fig. 9.과 같이 사용자의 ID(user number), STB 단말 정보, STB 기기의 MAC 주소, STB의 전원을 끈(sleep) 시간의 정보가 전송된다. 앞에서 설명한 STB Power On 시의 네트워크 패킷 내용과 결합하여 사용자의 서비스 이용 시간을 알 수 있다.

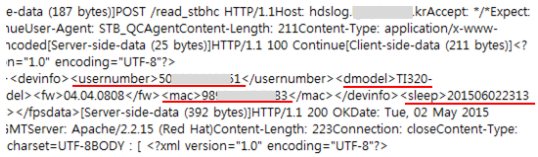

Fig. 9. Network packets when STB power off

3.2.4 문제점

본 논문에서 분석한 각 Use Case별로 전송되는 사용자의 개인정보와 각 개인정보의 프라이버시 침해 요인을 표로 정리하면 Table 7.과 같다. 방송사업자에서는 사용자 맞춤형 콘텐츠 제공을 목적으로 STB로부터 전송되는 사용자의 모든 이용 기록을 저장하고 사용자의 성향을 분석한다. 이러한 사용자 이용 기록의 수집 및 분석은 유출시 사용자의 사생활 침해로 이어진다. 또한 STB로부터 전송되는 데이터가 암호화되지 않은 평문 상태로 전송되기 때문에 해킹이나 Sniffing과 같은 외부로부터의 보안 위협에 노출되어 있다.

개인정보보호법 제 23조에 따르면 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 민감정보로 정의하고 있으며, 민감정보에 대해서는 별도의 동의를 받아야 한다고 명시되어 있다[8]. 성인 콘텐츠 이용시, 서비스 이용 기록은 개인의 성적 취향과 관련된 민감정보에 해당한다. 그러나 이러한 민감정보를 포함한 사용자의 개인정보가 STB를 통해 방송 사업자에게 전송되고 있음에도 불구하고 그에 대한 알림이나 별도의 동의 절차 없이 진행되기 때문에 사용자는 정보의 주체인 자신도 모르는 사이 정보가 노출되고 분석되고 있는지에 대한 인식조차 없는 문제가 발생한다.

Table 7. User's personal information transferred in each use step and Privacy Risk

Step	Collected information	Transfer Information	Included in subscription agreement	Illegality	Privacy Risks
STB Power On	User and device information	User number			Personal information exposure
		STB device information(Model number, MAC / IP address)			Using the appliance vulnerability attack risk
		STB power-on time	Not included		Personal privacy exposure
	Channel information and user rights	Full channel list	Not included		
		User rights for pay-per-view channels (including adult channels)	Not included	O	**Sensitive information** (Adult content using record) collection
Changing Channel	Channel / Program information	User number, STB MAC address			Personal information exposure
		Channel information	Not included		Targeted attacks through personal propensity analysis
		Program information	Not included		Targeted attacks through personal propensity analysis
VOD play	VOD viewing / purchasing information	User number, STB MAC address			Personal information exposure
		VOD information	Not included	O	**Sensitive information** (Adult content using record) collection
		VOD validity	Not included		
Run web application	App usage information	User number, STB MAC address			Personal information exposure
		Website visit history (time, web address)	Not included		Targeted attacks through personal propensity analysis
STB Power Off	User and device information	User number			Personal information exposure
		STB device information(Model number, MAC / IP address)			Using the appliance vulnerability attack risk
		STB power-off time	Not included		Risk of personal privacy exposure

IV. 사용자 개인정보 보호방안

4.1 서비스 가입동의서

개인정보보호법에 따르면, 개인정보의 처리에 관한 동의 여부와 동의 범위는 정보의 주체가 직접 선택하고 결정할 권리가 있다. 그러나 국내 IPTV 서비스의 경우, 소비자가 서비스 가입을 하는 과정에서 개인정보의 항목 전체를 한 개의 항목으로 통합하여 일괄 동의로 이루어지며, 사용자가 선택할 수 있는 관련 선택지는 '동의함'과 '동의하지 않음' 둘 중 하나이다. 사업자에서 제시한 사항에 동의하지 않을 경우, 서비스를 이용할 수 없는 제약이 발생한다. 사실상 동의를 거부할 권리가 실현되지 않는 상황이다. 결국, 사용자는 본인의 의사와는 다르게 사업자에서 요구하는 방향으로 선택을 할 수밖에 없고, 이는 매우 형식적인 절차로 전락하여 실질적으로 소비자에게 선택할 권리를 보장한다고 할 수 없다. 따라서 현재 IPTV 서비스 가입시, 가입신청서 상에서 개인정보 수집항목 전체를 일괄로 묶어서 수집 동의를 구하는 방식에서 탈피하여 각 서비스 및 콘텐츠에서 수집되는 개인정보 항목을 세분화하고 사용자가 직접 개인정보의 수집 범위를 설정하도록 개선되어야 한다. 또한 개인정보 항목을 필수 동의 항목과 선택 동의 항목으로 구분하여야 한다. 수집되는 개인정보의 범위를 사용자가 직접 선택할 수 있도록 하고, 민감정보, 고유식별번호와 같이 별도 동의가 필요한 항목을 별도 동의 항목으로 구분하여야 한다. 이렇게 함으로써 사용자에게 개인정보의 제공에 동의함에 있어 정보주체가 가져야 하는 개인정보의 열람권, 개인정보 수집 철회권, 거부권 등의 권리를 보장해 주어야 한다. 다음 Table 8.은 개인정보보호종합포털에서 권고하는 개인정보 동의 양식이다[11]. IPTV 서비스 가입동의서에서도 이러한 방식으로 사용자의 동의를 구함으로써 쉬운 설명과 고지를 통해 사용자의 개인정보가 어떤 용도로 사용되는지 쉽게 알릴 수 있고, 필수적 동의사항과 선택적 동의사항을 정확히 구분하여 제시하고, 선택적 동의사항에 동의하지 않는 경우에도 서비스 이용에 제한이 없음을 밝혀 선택권을 보장할 수 있도록 해야 한다.

4.2 IPTV STB에서의 개인정보 범위 설정

STB 내에서는 사용자의 개인정보 전송에 대한 범위를 사용자가 직접 설정하는 기능이 제공되어야 한다. 영국의 통신사 British telecom의 경우, Fig. 10.과 같이, 홈페이지를 통하여 사용자의 개인정보 수집 관련하여 사용자가 선택할 수 있는 선택 항목들을 제공한다. 선택 항목은 3가지 단계로 구분되어 있으며, 단계별로 수집하는 개인정보의 범위가 달라진다. 사용자는 방송사업자에서 수집하는 개인정보의 범위와 수준을 직접 선택함으로써, 자신의 개인정보에 관한 보호조치를 스스로 할 수 있게 되는 것이다. 국내 IPTV 서비스에서도 STB를 통해 서비스를 이용하는 과정에서 언제든지 사용자가 설정을 변경하여 본인의 개인정보에 대한 관리를 스스로 설정하고 관리할 수 있도록 해야 한다. 다음 Table 9.는 개인정보의 중요도에 따른 정보공개 단계를 구분하고, 각 단계에서의 예시와 프라이버시 위험도에 대해 구분한 표이다. 레벨 1은 시청정보 중 시청 이력만을 취급하고, 이용자 정보는 다루지 않는다. 이 레벨에서 수집할 수 있는 정보는 익명의 정보이며, 콘텐츠의 인기도를 측정하기 위한 시청률 수집 정도의 정보 수집이 가능하다. 레벨 2는 시청자의 성별, 연령, 가족 구성, 지역등의 정보까지 다룬다. 이러한 정보는 콘텐츠의 시청 이력과 같은 정보와 결합하여 더 많은 개인 정

Table 8. Example for Personal Information Collection and Usage Agreement

essential consent information		
Personal Information	purpose of collecting and usage personal information	Period of possession and use of personal data
name, email address,	Personal identification, delivery notices, new product introduction	delete with secession
agree ☐	not agree ☐	
selective consent information		
Service usage history, access log	Seamless and always-on services, dispute resolution	delete After three months from the Members withdrawal date
agree ☐	not agree ☐	

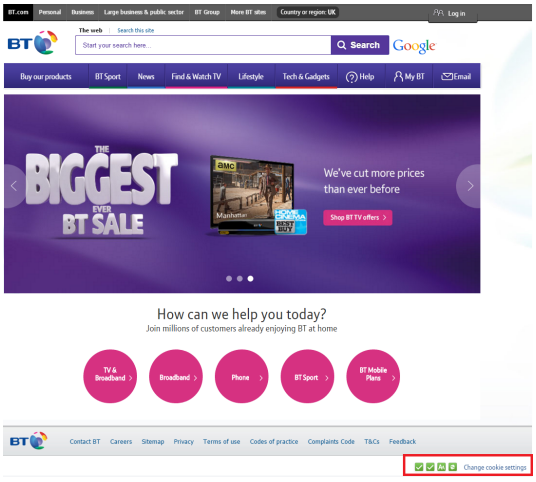

Fig. 10. Example for changing privacy level setting: British Telecom

보의 수집과 활용이 가능하다. 예를 들어, 한 프로그램의 시청자 중 여성의 비중이 많다는 것을 이용하면 여성을 위한 광고를 동시에 방송할 수 있다. 레벨 3은 시청자의 개인 식별 정보까지 취급한다. 예를 들면, 이름이나 메일 주소에 대한 정보가 포함되는데, 이 레벨의 이용자 정보와 시청 이력을 다루는 것으로, 그 시청자에 대한 직접적인 식별이 가능해진다. 레벨 3의 정보를 다루지 않더라도 레벨 1에서도 기존 TV의 시청률과 비교해 IPTV의 시청정보를 이용하여 정확한 정보를 수집할 수 있다는 점에서 레벨 1이라고 해도 개인정보에 해당하므로, 정보를 수집하는 경우에는 이용자의 허가를 얻을 필요가 있다. 이밖에도 수집되는 개인정보의 활용 목적 및 활용 현황, 폐기 여부에 대해 실시간으로 사용자에게 알림이 가는 기능이 제공되어야 한다. 방송 시청 중 팝업 알림 서비스, SMS, e-mail을 통한 사용자 알림 서비스와 같은 실시간 정보를 제공하여 사용자가 자신도 모르는 사이 본인의 개인정보가 오·남용되는 사고를 예방할수 있도록 해야 한다. 이를 통해 방송 서비스 이용을 위한 최소한의 정보가 수집되도록 하여, 개인정보가 유출되더라도 그로인한 피해를 최소화할 수 있다.

V. 결론 및 향후 과제

본 논문은 사용자수가 지속적으로 증가하고 있는 국내 IPTV 서비스에서 방송사업자가 수집하는 사용자의 개인정보에 대한 실태를 분석하고 문제점을 도출하였다. I사의 IPTV 서비스를 대상으로 먼저 서비스 가입신청서 상에서 사용자에게 개인정보 수집 동의를 받는 과정에서 형식적인 사용자의 동의가 이루어지고 있는 실태에 대한 문제점을 제시하였다. 또한 안드로이드 운영체제 기반인 IPTV STB의 네트워크 패킷을 분석함으로써 STB를 통해 실제로 사용자의 어떤 개인정보가 방송사업자에게 전달되는지를 보였다. 그 결과 서비스 이용 시간, 시청한 채널과 방송, 구매한 VOD, 방문한 웹사이트와 같이 사용자의 성향을 알 수 있는 데이터를 얻을 수 있었다. 획득한 데이터의 분석을 통해 전송되는 사용자의 개인정보의

Table 9. Leveling of transferred Personal Information

	Level 1	Level 2	Level 3
Personal Information collected	User's viewing history only (no information on what the user is authorized)	Viewing history and information about any user authorized (attribute information)	Viewing history personally identifiable information (e-mail address, etc.)
Data example	Terminal Type "003" in the channel 228. being watched by anonymous users from 12:00 to 15:30	Terminal Type "003" in the channel 228. being watched by female users from 12:00 to 15:30	Terminal Type "003" in the channel 228. being watched by hong gil dong (e mail : hgd:iptv.net) from 12:00 to 15:30
The consent of the user	necessary	necessary	necessary
Privacy Risk	Low (Because it can not identify the individual)	Low (Because it can not identify the individual)	High(Because it is a personally identifiable information)

범위와 선택권을 사용자가 직접 선택할 수 없고 일방적으로 수집되고 있음에 대한 문제점을 제시하였고, 마지막으로 제시한 문제점에 대해 사용자의 개인정보를 보호할 수 있는 방안을 제시하였다.

향후에는 본 논문에서 제시한 문제점과 사용자 개인정보보호 방안에 대해 실제 서비스에서 구현 가능한 IPTV에서의 개인정보보호 플랫폼에 관한 연구를 진행하고, 국내 서비스 뿐만이 아닌 해외 서비스를 대상으로 연구 범위를 확대하여 STB를 통해 전송되는 개인정보의 암호화, 익명화와 같은 기술적인 보호 방안에 관한 연구를 진행할 예정이다.

References

〔1〕 KTB Investment & Securities Report, "Pay- TV", Apr. 2015.

〔2〕 Yong-joon Choi, "Digital interactive services - Focusing on the operating model and business model navigation Research", commbooks, 46, World Cup buk-ro, Mapo-gu, Seoul, Korea, pp. 167, Mar. 2003.

〔3〕 BBC News, "LG investigates Smart TV 'unauthorised spying' claim", Nov. 2013. (http://www.bbc.com/news/technology-25018225)

〔4〕 ITU, FG IPTV: "DOC-0181: IPTV Architecture", pp. 8, Jan. 2015.

〔5〕 ITU, FG IPTV: "DOC-0191: IPTV Related Protocols", pp. 8-10, Jan. 2015.

〔6〕 ITU, FG IPTV: "DOC-0182: Service scenarios for IPTV", pp. 7-8, Jan. 2015.

〔7〕 Constitution of the Republic of Korea, "PERSONAL INFORMATION PROTECTION ACT", Law No. 13423, Jul. 2015

〔8〕 Constitution of the Republic of Korea, "ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.", Law No. 13344, Jun. 2015

〔9〕 Understanding Port Mirroring (http://www.juniper.net/techpubs/en_US/junos12.3/topics/concept/port-mirroring-qfx-series-understanding.html)

〔10〕 About Wireshark (https://www.wireshark.org/)

〔11〕 Privacy Information Protection Portal (http://www.privacy.go.kr/)

〈저자소개〉

이 진 혁 (Jinhyuk Lee) 학생회원
2007년 2월: 아주대학교 산업정보시스템공학과 졸업
2016년 2월: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 개인정보보호, 보안성평가

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월: KISA(舊한국정보보호진흥원) 팀장
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화전문가
2004년 3월~2011년 2월: 성균관대학교 정보통신공학부 조교수, 부교수
2011년 3월~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보 차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~2009년: 전자 정부 서비스 보안 위원회 사이버 침해사고대응 실무위원회 위원
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2012년 3월~2012년 6월: 선관위 디도스 특별검사팀 자문위원
2013년 4월~2013년 12월: IT보안인증사무국 자문위원
2013년 9월~현재: 중앙선거관리위원회 자문위원
2014년 3월~현재: 헌법재판소 자문위원
2014년 9월~2015년 3월: 대한민국 육군사관학교 초빙교수
2014년 12월~현재: 다음카카오 프라이버시정책 자문위원
2015년 5월~현재: 코스콤 자문위원
2015년 6월~현재: 대검찰청 디지털수사 자문위원회 위원
2015년 6월~2015년 12월: IT보안인증사무국 인증위원회 인증위원
2015년 7월~현재: 방위사업청 방산기술보호 자문관
2016년 1월~현재: 한국정보화진흥원 전략과제심의위원회 위원
2016년 1월~현재: 전자정부지원사업 심의위원회 위원
2016년 6월~현재: 2018 평창동계올림픽 조직위원회 정보보호전문위원회 전문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security