블록체인 상의 영장 전달을 통한 연속적인 합법적 감청

이정빈*, 인호*
*고려대학교 컴퓨터학과
e-mail:{jungbini, hoh_in}@korea.ac.kr

Delivering Warrants Model using Blockchain for Seamless Lawful Interception

Jung-Been Lee*, Hoh Peter In*
*Dept of Computer Science, Korea University

요 약

합법적 감청(LI: Lawful Interception)이란, 합법적으로 음성 통신 내용 및 데이터와 그와 관련된 일련의 정보를 수집하는 활동을 말한다. 그러나 IP 기반의 4G-LTE 네트워크와 다수의 사업자망을 이동하는 과정에서 발생되는 반복적인 법원의 영장 재발부 절차는 합법적 감청의 연속성을 저해하는 요소가 되어왔다. 이러한 문제점을 해결하기 위해 재발부 과정을 생략하고, 기존 영장 그대로 다음 국가나 네트워크 사업자에게 전달하는 방식이 제안되었지만, 보안성에 대한 문제가 여전히 존재한다. 본 연구에서는 블록체인 기반의 분산 데이터베이스 상에서 디지털 영장을 발부함으로써 영장의 재발부 과정을 거치지 않으면서도 보안성이 높고 안전하게 연속적인 합법적 감청을 수행할 수 있는 모델을 제안한다.

1. 서론

합법적 감청이란, 합법적으로 개인의 음성 통신 내용 및 데이터, 그리고 그와 관련된 일련의 정보에 대한 공식적인 접근이 인가된 감청 활동을 말한다. 합법적 감청 수행 도중 감청 타겟의 지역이나 국가 또는 사용하는 네트워크 사업자가 변경 될 때마다, 해당 사법집행기관(LEA: Lawful Enforcement Agencies)으로부터 공식적 감청을 위한 영장 재발부 프로세스가 필요하다[1]. 이는 연속적인 합법적 감청을 저해하는 요소이며, 이를 악용한 국제 테러 및 각종 범죄의 사전 탐지나 사후 추적을 어렵게 만들고 있다.

이러한 문제점을 보완하기 위해, 영장을 재발부하지 않고 중간에서 그 권한을 심사하고 전달하는 Trust Third Party(TTP)나 LI 서버의 개념[2] 및 유럽전기통신표준협회(ETSI: European Telecommunications Standards Institute)의 LI 표준 참조 모델에서 제시하는 Dynamic Triggering[3,4]을 통해 즉시 다른 사업자에게 영장의 권한을 전달하는 방법 등이 제안되었다. 그러나 이러한 방법은 영장이 네트워크상에 전달되는 과정에서 공격자에 의해 악의적으로 변조되거나, 관련 서버들이 공격당할 수 있는 문제점을 여전히 가지고 있다.

본 연구에서는 이러한 문제점을 해결하기 위해, 블록체인 기반의 분산 데이터베이스 상에 안전하고 보안성이 높은 디지털 영장 전달 모델을 제안한다.

2. 기존 ETSI 참조 모델 영장 발부 절차

기존에 다양한 영장 전달 기법[2,3,4]이 제안되었으나, 여전히 LEA로부터 영장을 재발부 해야 하는 프로세스로 인해 연속적인 감청의 공백이 생기는 문제를 해결할 수 없었다. 그림 1은 ETSI의 표준 참조 모델[5]에 기반 한 감청 절차에 표현하고 있다.

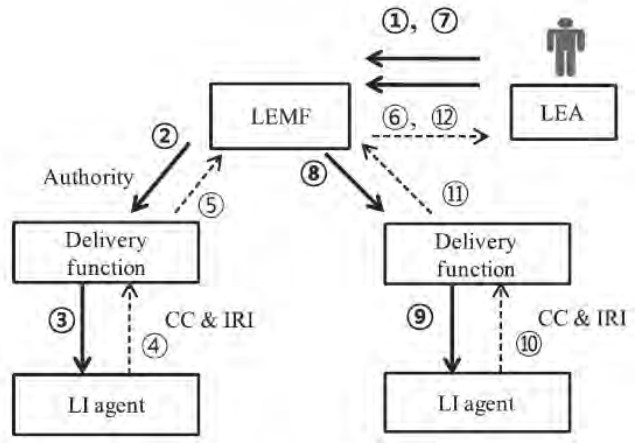

그림 1. ETSI 참조 모델 기반 합법적 감청 절차[2]

초기 영장 발부가 진행 된 후(①-③), 감청 정보(CC: Contents of Communications, IRI: Intercept Related Information)를 Delivery function을 거쳐 LEMF(Lawful Enforcement Monitoring Facility) 전달한다(④-⑥). 만약 감청 타겟(LI agent)이 또 다른 목적지로 이동하면서 물리

적인 위치 또는 네트워크 사업자가 변경되면 다시 LEA로부터 영장을 재발부하는 절차(④-⑥)을 거쳐야 한다. 그 후 다시 감청 타겟의 감청이 시작(⑩-⑫)되나, 추가적인 영장 재발부 과정이 필요하고 전달되는 영장의 보안성과 다른 연구에서 제시되는 영장 권한 심사 및 전달 서버의 공격에 대한 대안은 고려되지 않는다.

3. 블록체인 기반 영장 전달 모델

블록체인(Blockchain)[5]은 분산 데이터베이스의 한 형태로 위변조가 불가능한 가치 정보가 담긴 블록이 지속적으로 연결되어 P2P 네트워크상에 배포된다.

그림 2는 본 연구에서 제안하는 블록 체인 기반 영장 발부 모델을 나타내고 있다.

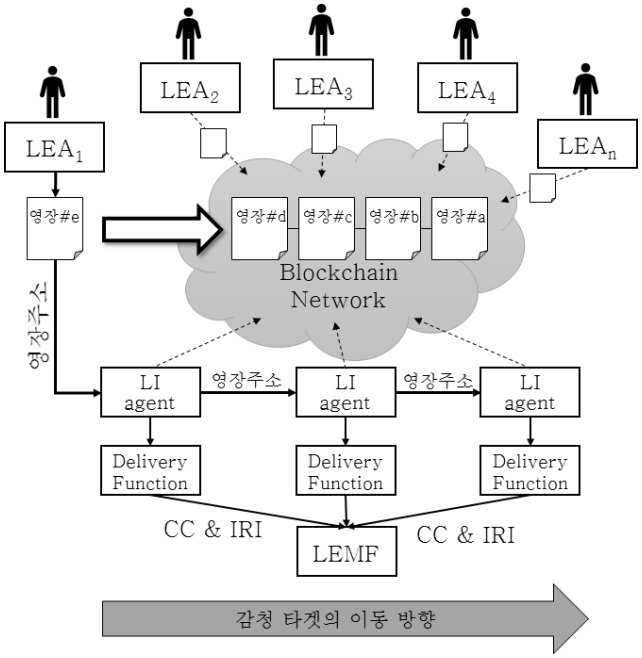

그림 2. 블록체인 기반 영장 전달 모델

LEA는 발부한 영장을 바로 LEMF에 전달하지 않고, 블록체인 기반 네트워크에 전송하여 영장블록으로 추가하고 추가된 영장블록의 주소만 LI agent에 전달된다. 최초 LEA로부터 영장 주소를 전달받은 LI agent는 영장에 대한 정보를 블록체인 네트워크에 접속하여 전달받고 합법적 감청을 실시한다. 만약 감청 타겟이 다른 지역이나 사업자로 이동할 경우, 다음 LI agent는 다시 LEA로부터 영장을 재발부 받지 않고 이전 LI agent로부터 영장주소만 전달받아 블록체인의 영장을 조회한다. 기존 LI 표준 모델에 기반한 영장 재발부 과정이 생략되기 때문에 연속적인 LI를 수행할 수 있다.

이러한 블록체인의 특성을 활용한 LI 영장 전달 모델의 장점은 아래와 같다.

- 블록체인의 작업증명(Proof-of-work) 기술을 이용하여 위변조가 불가능하기 때문에 악의적인 의도를 가진 공격자가 영장을 전달하는 과정에서 영장을 조작할 수 없다.
- 분산 네트워크상에 있는 모든 노드에 동일하게 영장이 저장되어 있기 때문에 LI 서버나 TTP 같은 단일 서버가 공격을 받아도 영장 전달에 차질이 발생하지 않는다.

4. 결론

기존 ETSI 표준에서 제시하고 있는 LI 영장 발부 절차는 감청 타겟의 위치 및 사업자의 변경에 따라 영장을 재발부해야 하기 때문에 연속적인 감청이 어렵다. 또한, 기존 연구로 제안된 영장 전달 방식은 영장에 대한 안정성을 보장하지 않고, 영장 심사 및 전달 역할을 하는 서버의 공격에 대한 대안이 미비하다.

본 논문에서는 이러한 문제점들을 해결하고자, 블록체인 기반의 LI 영장 전달 모델을 제안하였다. 블록체인의 특성을 이용하였기 때문에 영장이 전달되는 과정에서 위/변조하기 불가능하고, TTP나 LI 서버들이 공격받게 되면 전체 LI 수행이 마비되는 것과는 달리 분산 데이터베이스상에 영장이 저장되어 있기 때문에 하나의 노드가 공격을 받아도 끊임없이 연속적으로 LI를 수행할 수 있다.

사사

이 논문은 2016년도 정부(미래창조과학부)와 정보통신기술진흥센터 재원으로 한국연구재단-차세대정보·컴퓨팅기술개발사업(2012M3C4A7033345) 및 대학 ICT연구센터 육성·지원사업(IITP-2016-R0992-16-1011)의 지원을 받아 수행된 연구임.

참고문헌

[1] ETSI, ES 201 671: Telecommunications Security; Lawful Interception(LI); Handover interface for the lawful interception of telecommunications traffic, 2007.

[2] Lee, Myoungrak, et al. "A seamless lawful interception architecture for mobile users in IEEE 802.16 e networks." Journal of Communications and Networks 11.6, p.626-633, 2009

[3] Kim, Dohoon, et al. "3G IP Multimedia Subsystem based framework for lawful interception." annals of telecommunications-annales des télécommunications 69.7-8, p.347-361, 2014

[4] 이명락, 이정빈, 한영섭, "SIP/IMS Service Mobility 탐지를 통한 Lawful Interception Dynamic Triggering 기법에 관한 연구', 한국정보처리학회, VOL.22(02), p. 606-609, 2015. 10.

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system.", 2008