IoT 환경에서 상류 통신의 프라이버시 보호 레이어 개념1)

한인국*, 연재환*, 이해영*, 김형종**
*청주대학교 디지털보안전공
**서울여자대학교 정보보호학과
e-mail:hkim@swu.ac.kr

Concept of a Layer for Privacy Protection of Upstream Communications in IoT Environments

In Gook Han*, Jae Hwan Yeon*, Hae Young Lee*, Hyung-Jong Kim**
*Major in Digital Security, Cheongju University
**Dept of Information Security, Seoul Women's University

요 약

본 논문에서는 스마트폰에서 사물인터넷 기기로부터 수집한 데이터를 사물인터넷 서버로 전송할 때 프라이버시 보호를 지원할 수 있는 상류 프라이버시 보호 레이어를 제안한다. 제안 레이어는 프라이버시 정책에 따라 서버와 직접 연결, 프록시를 통한 연결, 가상사설망을 통한 연결, 그리고 익명 네트워크를 통한 연결을 동적으로 변경할 수 있고, 이를 통해 데이터 전송 효율의 저하를 최소화하면서도 프라이버시를 보호할 수 있다.

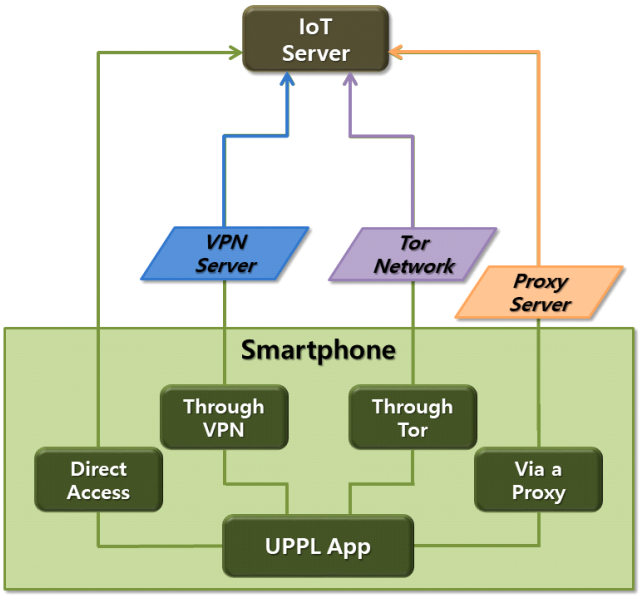
1. 서론

많은 사물인터넷(Internet of Things; 이하 IoT) 기반 서비스에서, 스마트폰은 IoT 기기와 서버 사이의 중계자 역할을 하고, 이에 따라 이들 간의 통신으로 인한 프라이버시 침해가 발생할 수 있다[1]. 프라이버시 보호 레이어(privacy protection layer; 이하 PPL)[2,3]는 IoT 기기에서 수집된 감지 데이터를 정책에 따라 선택적으로 암호화 및 전송하는 레이어를 제공한다. 그러나 PPL 모듈을 설치하기 불가능한 경우(예를 들어, 국외 서비스)에는 프라이버시 보호가 어렵다. 또한 통신 중 익명성을 보장하지 못하여 프라이버시 침해가 발생 소지도 있다[4].

본 논문에서는 스마트폰 및 서버 간의 통신 중 프라이버시 보호를 위한 상류 프라이버시 보호 레이어(upstream privacy protection layer; 이하 UPPL)를 제안한다. UPPL은 정책에 따라 직접 연결, 가상사설망(virtual private network; 이하 VPN), 또는 Tor 익명 네트워크[5]를 통해 감지 데이터를 전송한다. 현재 직접 및 Tor 네트워크 기반 연결을 지원하는 개념 증명 코드까지 개발하였다.

2. 상류 프라이버시 보호 레이어(UPPL)

UPPL은 IoT 기기들로부터 수집된 감지 데이터를 프라이버시 정책에 따라 안전하게 상류(즉, 스마트폰과 서버 간의 통신)로 전송하는 것을 목적으로 한다. PPL의 서버 설치 여부와 상관없이, 스마트폰과 서버 간의 다양한 연결을 지원하여 프라이버시 보호 목적에 부합하는 전송 서비스를 제공한다. 프라이버 보호 수준에 맞춰 통신 방식을 변경함으로써 통신 효율 저하를 최소화하면서 프라이버시를 보호할 수 있다.



(그림 1) UPPL 개념도

(그림 1)은 UPPL의 개념도를 보인다. UPPL는 서버와의 직접 연결, 프록시를 통한 연결, VPN을 통한 연결, Tor 익명 네트워크를 통한 연결을 지원한다. Tor 네트워크와의 연결은 Orbot을 이용한다. IoT 기기들로 부터 수

1) 이 연구는 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2017R1D1A1B03034644).

집된 감지 데이터는 PPL의 프라이버시 보호 정책에 따라 분류되고, UPPL로 전달된다. 정책에 따라 프라이버시 침해 소지가 있는 민감한 데이터의 경우, VPN 또는 Tor 네트워크를 통해 IoT 서버에 전송된다. Tor 네트워크는 트래픽 자체만으로도 프라이버시 침해가 발생할 수 있는 데이터 전송에 활용된다. 예를 들어, 홈 메디컬 기기로부터 수집된 데이터는 전송 자체만으로도 프라이버시 침해가 가능하므로[4], Tor 네트워크를 통해 전달되도록 정책을 설정할 수 있다. 수집된 데이터가 이미 암호화된 경우나 굳이 암호화할 필요가 없는 경우에는, 정책에 따라 서버와 직접 연결되거나 프록시를 통해 연결된다. 이를 통해 통신 효율을 증대시킬 수 있다. UPPL은 이와 같은 정책 기반의 통신 방식 변경을 통해 통신 효율의 저하를 최소화하면서도 프라이버시를 보호할 수 있다.

3. 구현

UPPL의 일부 연결을 지원하는 개념 증명(proof-of-concept)을 개발하였다. UPPL 구현에서 가장 중요한 점은 다양한 연결 방식을 지원하는 하는 것이다. Tor 네트워크 연결 및 VPN 연결을 위해서는 구글 플레이스토어에서 제공되는 외부 앱을 사용하였다. 앱 단위로 연결 방식을 지정할 수 있다는 점에 착안하여, 각각의 연결 방식을 실제 수행하는 보조 앱들과 최종 사용자 앱들과 연결되는 중앙 처리 앱으로 구성하였다. 중앙 처리 앱은 최종 사용자 앱들로부터 전달받은 IoT 데이터를 PPL 정책에 따라 해당 보조 앱들에게 전달한다. 각 보조 앱은 중앙 처리 앱으로부터 받은 데이터를 해당 연결 방식을 통해 IoT 서버로 전송한다. 예를 들어, 민감한 정보는 익명 네트워크를 통해 전송되도록 PPL 내에서 정책으로 설정되어 있다면, 해당 정보는 Tor 네트워크를 통해 서버에 전송된다.

현재 버전에는 VPN 연결과 Tor 네트워크 연결을 동시에 지원하지 않으며, 사용자 선택(즉, 프라이버시 정책)에 따라 설정하여 양자 중 택일하여 사용할 수 있다. 향후 VPN 연결 및 Tor 네트워크 연결을 모두 지원할 수 있도록 전송 시간을 스케줄링하는 기법을 적용할 계획이다.

4. 결론 및 향후연구

본 논문에서는 IoT 환경에서 발생할 수 있는 프라이버시 침해 문제를 완화하기 위한 UPPL을 제안하였다. UPPL은 스마트폰과 IoT 서버 간의 데이터 통신 중 프라이버시 보호를 다룬다. IoT 서버에 PPL의 적용이 어려운 경우, PPL은 UPPL로 감지 데이터를 전달하고, UPPL은 정책에 따라 다양한 연결 방식을 통해 IoT 서버에게 데이터를 전달한다. 이를 통해 전송 효율을 유지하면서도 프라이버시를 보호할 수 있다.

향후에는 PPL과 UPPL을 통합하는 것을 1차 목표로 하고 있다. 또한, 앞서 언급한 바와 같이, 다양한 연결 방식을 지원하기 위한 스케줄링 기법에 대해서도 연구할 계획이다. 마지막으로 프라이버시 보호 관점에서 성능 평가도 수행할 계획이다.

참고문헌

[1] Y. Zhou *et al.*, "Taming Information-stealing Smartphone Applications (on Android)," Proc. of TRUST, 2011.

[2] H.J.. Kim and H.Y. Lee, "A Study on the Privacy Protection Layer for Android IoT Services," Proc. of ICSSA, 2018.

[3] 박화현 외, "AndroidThings 환경의 정보보호 방안 연구," 한국시뮬레이션학회 학술대회논문집, 2018.

[4] 이해영, 김형종, "사물인터넷 프라이버시 트래픽 보호를 위한 가정용 게이트웨이 개념," 한국통신학회 학술대회 논문집, 2017.

[5] Tor Project. https://www.torproject.org/

[6] Orbot: Tor for Android. https://guardianproject.info/apps/orbot/