한국컴퓨터정보학회 동계학술대회 논문집 제28권 제1호 (2020. 1)

트래픽 자동 분류 기반의 상류 프라이버시 보호 계층 개발

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

Development of a Upstream Privacy Protection Layer Based on Traffic Classification

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

● 요 약 ●

홈/개인 IoT 환경에서 모바일 기기나 유무선 공유기는 IoT 기기의 트래픽을 중계하는 경우가 많다. 본 논문에서는, 홈/개인 IoT 환경에서 IoT 기기들이 서버로 전송한 패킷들을 프라이버시 보호 측면에서 더 안전하게 상류로 전송하는 기능을 제공하는 트래픽 자동 분류기반의 상류 프라이버시 보호 계층을 제안한다. 트래픽의 목적지 주소를 기반으로, 직접 연결, 프락시를 통한 연결, VPN을 통한 연결, Tor 익명 네트워크를 통한 연결 방식 중 하나를 선택하고, 선택된 연결 방식으로 상류로 패킷을 전달한다. 별도의 사용자 인터페이스를 통해 목적지 주소 및 적합한 연결 방식을 설정할 수 있다. 제안 계층은 모바일 기기 및 유무선 공유기에 적용 가능하며, 현재 모바일 기기용 개념 증명 예제를 구현하였다.

키워드: 프라이버시(privacy), 사물인터넷(Internet of things), 보안(security)

I. Introduction

많은 경우, 모바일 기기 및 유무선 공유기는 IoT 기기와 서버를 연결하는 중계자가 되며, 프라이버시 침해가 주로 발생하는 '약한' 노드가 될 수도 있다[1]. 프라이버시 보호 계층(privacy protection layer; PPL)[2]은 모바일 기기에서 상·하류 통신 보호를 위한 계층을 제공하지만, PPL이 제공하는 SDK를 이용하여 IoT 기기와 서버를 개발·수정해야 하는 문제를 가진다. 상류(upstream) 프라이버시 보호 계층(UPPL)[3]은 상류 통신 프라이버시 보호를 위한 다양한 연결 방식을 지원하나, 사용자가 또는 IoT 기기 제조사에서 연결 방식을 직접 선택해야 하는 문제를 가진다.

본 논문은 목적지 주소를 기반으로 트래픽을 자동 분류하여 적합한 통신 연결 형태로 상류로 전달하는 트래픽 자동 분류(traffic classification) 기반의 상류 프라이버시 보호 계층(TC-UPPL)을 제안한다. 제안 계층은 목적지 주소별로 연결 방식을 정의한 정책을 기반으로, 직접, 프락시(proxy), VPN, Tor 익명 네트워크[4] 연결을 통해 트래픽을 상류로 전송한다. TC-UPPL 개념 증명 예제도 함께 설명한다.

II. Proposed Layer

1. Previous Work

UPPL[3]은 IoT 기기와 서버 간의 통신 연결 방식을 다양하게 선택할 수 있는 계층으로, 직접 연결, 프락시를 통한 연결, VPN을 통한 연결, Orbot[5]을 이용한 Tor 익명 네트워크 연결 방식을 제공한다. 전송하는 데이터의 특성 및 외부 상황에 따라 통신 방식을 선택할 수 있으므로, 이를 통해 프라이버시 침해가 우려되는 데이터 또는 트래픽을 보호하면서도 그렇지 않은 데이터 또는 트래픽에 대해서는 통신 효율 저하를 방지할 수 있다. 그러나 연결 방식을 사용자 또는 개발자가 직접 선택해야 한다는 문제를 가진다.

2. Overview of the Layer

TC-UPPL은 기존 UPPL의 단점을 개선한다. 사용자가 수작업으로 연결 방식을 설정하는(또는 개발자가 사전에 지정하는) 기존의 UPPL과는 달리, TC-UPPL은 사전에 정의된 정책에 따라 트래픽을 자동 분류하여 적합한 연결 방식을 설정한다. 정책은 데이터 및 트래픽의

목적지 IP 주소를 기준으로, 프라이버시 침해 가능성을 고려하여 설정한다. 이에 따라 사용자가 수작업으로 연결 방식을 설정할 필요가 없으며, IoT 기기 제조사는 TC-UPPL 서비스 제공자에게 목적지 IP 주소 및 적합한 연결 방식을 제공하면 된다. 또한, 제조사에서 이를 제공하지 않더라도, 서비스 제공자가 데이터 및 트래픽을 분석하여 정책을 설정할 수도 있다.

3. Traffic Classification Policy

현재 TC-UPPL의 트래픽 자동 분류 정책은 가장 기본이 되는 트래픽의 목적지(IoT 기기 → 서버) IP 주소를 기준으로 연결 방식을 설정하도록 설계되었다. 즉, IoT 기기로부터 받은 패킷의 목적지 IP에 따라 통신 방식이 선택되고, 해당 패킷은 선택된 연결 방식으로 상류로 전달된다.

추후 IoT 기기의 MAC 주소, 데이터 크기, 전송 주기 등 다른 기준의 추가도 가능하다. TC-UPPL은 IoT 기기의 게이트웨이 역할을 하는 모바일 기기나 유무선 공유기에 탑재되는 것을 가정하므로, 이러한 정보의 수집이 가능하다.

III. Implementation

구현한 TC-UPPL 개념 증명 예제는 IP 주소 기반 트래픽 분류를 담당하는 TC 모듈과 실제 다양한 연결 방식을 제공하는 UPPL 모듈로 나뉜다.

TC 모듈은 정책 관리를 위해 데이터베이스를 사용하였으며, 등록 사용자 인터페이스를 통해 IoT 기기 여부, 목적지 IP 주소 또는 URL, 연결 방식 등을 설정할 수 있다. 목적지 IP 주소는 테이블의 기본 키로 사용된다. 반환 인터페이스를 통해 특정 목적지 IP 주소에 적합한 통신 방식을 얻어올 수 있다.

UPPL 모듈은 다양한 연결 방식을 지원하는 것을 우선시한다. Orbot 및 Hola VPN[6]과 같은 외부 앱을 사용하여 Tor 및 VPN 연결 방식을 구현하였다. IoT 기기의 트래픽이 아닌 경우, 직접 연결을 통해 패킷을 전달하도록 하였다.

IV. Conclusions and Future Work

본 논문에서는 홈/개인 IoT 환경에서 IP 주소 기반의 트래픽 자동 분류를 통해 상류 통신 프라이버시를 보호할 수 있는 TC-UPPL을 제안하였다. IoT 기기가 전송한 패킷의 목적지 IP 주소를 기반으로, 4종의 연결 방식을 선택하여 상류로 전송함으로써, 전송 효율 저하를 최소화하면서도 프라이버시 보호도 제공할 수 있다.

앞으로는 트래픽을 분류하는 TC 모듈에 기계 학습 기법을 적용하여, 프라이버시 침해 가능 트래픽을 학습 및 자동으로 분류할 수 있도록 개선할 계획이다. 또한, 실제 프라이버시 보호 수준도 이론적/실험적으로 평가할 계획이다.

ACKNOWLEDGEMENT

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

REFERENCES

[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] I.G. Han et al., “Concept of a Layer for Privacy Protection of Upstream Communications in IoT Environments,” *Proc. of KIPS Fall Conference*, 2019.

[4] Tor Project. *https://www.torproject.org/*

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

[6] Hola Free VPN. *https://hola.org/*