Power Delivery Chip 기반의 은닉 채널

정혜림*,안성규*,박기웅†

세종대학교 시스템 보안 연구실*, 세종대학교 정보보호학과†

Covert Channel using Power Delivery Chip

Hye-Lim Jeong*,Sung-Kyu Ahn*, Ki-Woong Park†

*Department of Computer and Information Security, Sejong University.

요 약

하드웨어 디바이스의 발전이 급증하면서 은닉 채널 기술의 연구도 함께 발전하였다. 본 논문에서는 디바이스의 충전 모듈인 Power Delivery Chip과 디바이스 간에 은닉 채널을 제안한다. Power Delivery Chip은 디바이스로 전력 양을 조절하여 보낼 수 있도록 재설계를 통해 디바이스로 은닉 채널 신호를 전송하게 된다. 디바이스는 해당 은닉 채널의 신호를 수신하도록 수신 기능을 수행하는 악성코드를 감염시킨다. 제안과 함께 Power Delivery Chip과 디바이스로 스마트폰의 안드로이드에서 본 제안의 가능성을 설명하였다.

I. 서론

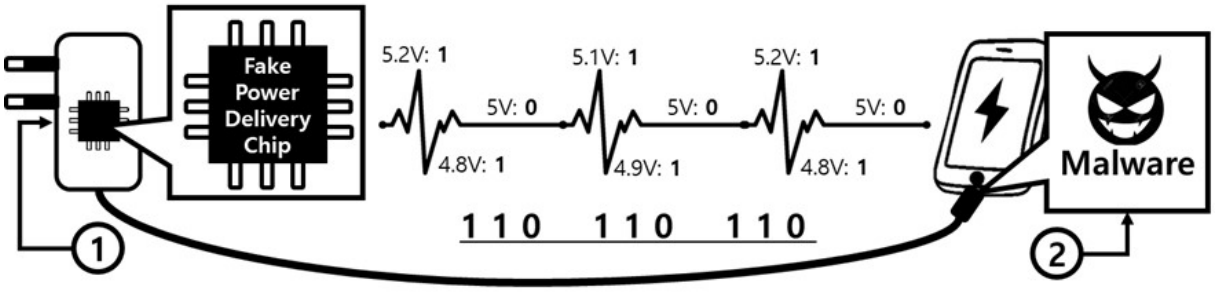
디바이스의 다양화와 사용률의 급증과 함께 은닉 채널 기술의 연구도 최근 많이 진행되고 있다. 은닉 채널 공격은 디바이스의 전력 소모 및 전자기파와 같이 누수 정보를 사용하여 디바이스를 침해하는 기법으로 일반적인 사용자들은 이러한 채널에 대해 인지하지 못한다. 이러한 은닉 채널 공격 기법으로 본 논문에서는 디바이스를 충전에 사용되는 USB 내 Power Delivery Chip을 이용한 은닉 채널 기법을 제안한다.

USB Power Delivery Chip(Power Delivery Chip)이란 USB에 연결된 기기의 전력을 전달하는 기능을 수행한다. 이 과정에서 해당 chip은 연결된 디바이스에게 전력의 양을 결정할 수 있다. 일반적인 충전 모드와 고속 충전 모드가 그 예이다. 최근엔 Power Delivery Chip 내 디바이스 인증 기능을 탑재하여 이 기능이 수행되면 데이터 송수신을 차단하기도 한다. 그러나 이러한 전력의 양을 결정할 수 있는 Power Delivery Chip을 조작하여 미세 전류를 조작한다면 디바이스로 특정 신호를 보낼 수 있는 은닉 채널을 제안한다.

본 논문에서 제안하는 USB 내 Power Delivery Chip을 이용한 은닉 채널 기법은 일반적으로 사용되는 Power Delivery Chip을 공격자가 신호를 보내도록 재설계해야 하며, 디바이스 내 전력의 양을 측정하고 이를 수정할 수 있도록 악성코드에 감염되어 있어야 한다.

II. Power Delivery Chip을 통한 은닉채널

본 논문에서는 디바이스의 USB Power Delivery Chip에 충전 전력의 양을 조절하여 디바이스로 신호를 전달하는 은닉 채널을 제안하였다. 해당 제안을 수행되기 위해서는 재설계된 Power Delivery Chip과 해당 은닉 채널의 수신



[그림 1] Power Delivery Chip 기반의 은닉 채널 디자인

지가 되는 악성코드가 필요하다. 이러한 은닉 채널의 구성은 그림 1과 함께 설명한다.

2.1 Power Delivery Chip

공격자는 디바이스에 연결될 Power Delivery Chip에 Chip 재설계로 신호를 입력한다. 입력의 신호는 그림 1과 같이 신호를 미세하게 조정을 하여 신호를 전송한다. 그림 1의 경우 5V의 충전량을 가정하고 작성하였다. 이와 같은 미세한 전류는 공격자가 어떤 신호를 전송하는지에 따라 전류 값이 달라지기 때문에 디바이스에서 전력을 상시 감시하더라도 패턴을 찾아내지 않는 이상 해당 은닉 채널을 탐지하기 어렵다. 본 논문에서 제안하는 설계에서는 5v에서 '0'이며, 그 외에서는 '1'로하여 설계하였으나 추후 연구로 실제 Power Delivery Chip을 설계하는 과정에서 일반적인 충전 상황의 전력의 범위에 따라 '1'의 신호 범위도 달라질 것이다.

2.2 디바이스 내 악성코드

스마트폰에서 안드로이드 프로그래밍으로 충전되는 전량을 측정할 수 있다. 안드로이드 프로그래밍을 위해 제공되는 BatteryManager 클래스를 사용하게 되면 전량의 미세한 차이 또한 측정 가능해진다. 그림 1과 같이 이러한 신호를 해석하여 신호로 변환한다면 은닉 채널에서 데이터를 송수신할 수 있을 것이다.

다른 디바이스에서도 전량을 측정할 수 있는 상황이 존재한다면 앞서 설명한 스마트폰 안드로이드 같은 경우와 같이 은닉 채널의 전량 신호를 측정하고 정보를 송수신할 수 있을 것이다.

III. 결론

본 논문에서는 은닉 채널로써 디바이스의 충전 모듈인 Power Delivery Chip에서 미세한 전량 조절을 통해 신호를 보내고 악성코드에 감염된 디바이스로 해당 신호를 수신하는 은닉 채널을 제안하였다. 추후 연구로는 본 제안의 은닉 채널을 구성하고 실험을 통해 검증할 것이다.

[참고문헌]

[1] ZHANG, Xiaosong, et al. A covert channel over volte via adjusting silence periods. IEEE Access, 2018, 6: 9292-9302.

[2] POOVENDRAN, Radha. No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices. In: Applied Cryptography and Network Security: 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings. Springer, 2017. p. 83.

[3] GURI, Mordechai; MONITZ, Matan; ELOVICI, Yuval. USBee: air-gap covert-channel via electromagnetic emission from USB. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016. p. 264-268.

[4] 조재범 기자. 삼성전자, 세계 최초 '전력제어+보안칩' 시스템LSI 내놔 ,2019,05,28,

ttp://biz.newdaily.co.kr/site/data/html/2019/05/28/2019052800016.htm 보안 뉴스

[5] NVDC I2C Battery Buck-Boost Charge Controller with System Power Monitor & Processor http://www.ti.com/lit/pdf/SLYY145?jktype=tech_docs

[6] BatteryManager, https://developer.android.com/reference/android/os/BatteryManager.html