블루투스 프로토콜의 보안 취약점에 대한 연구 동향

민현선, 이다은, 박경민* 김태훈■§, 방인규■

국립한밭대학교 지능미디어공학과, *한국전자통신연구원, §국립한밭대학교 컴퓨터공학과

{hsmin, delee}@edu.hanbat.ac.kr, *kmpark@etri.re.kr, {§thkim, ikbang}@hanbat.ac.kr

Research Trends in Security Vulnerabilities of the Bluetooth Protocol

Hyeonseon Min, Daeun Lee, Kyungmin Park*, Taehoon Kim■§, Inkyu Bang■

Dept. of Intelligence Media Engineering, Hanbat National University,

*Electronics and Telecommunications Research Institute,

§Dept. of Computer Engineering, Hanbat National University

요 약

본 연구에서는 Bluetooth Low Energy (BLE) 프로토콜의 구조적 취약점을 악용한 여러 종류의 무선 공격을 조사하고 실제 실험 환경에서 적용 가능성을 논의한다. 구체적으로 BtleJuice, GATTacker, Btlejack 등 대표적인 BLE 프로토콜 공격의 원리를 분석하여 링크 계층, SMP, GATT 계층의 보안 취약점을 확인하였다. 이를 통해 BLE 프로토콜의 근본적인 보안 취약점과 BLE 프로토콜의 사용이 AR 기기와 같은 실시간 응용 기기에 미치는 보안 위협을 논의한다.

Ⅰ. 서론

최근 스마트폰, 스마트워치, 무선 이어폰, 스마트 조명 등 다양한 전자기기들이 Bluetooth, WLAN 등 무선 통신 프로토콜을 기반으로 연결되며 우리의 일상생활은 더욱 편리해지고 있다. 특히 Bluetooth는 저전력 및 근거리 통신 특성을 바탕으로 모바일 기기 간의 데이터 전송, 주변기기 제어, 위치 기반 서비스 등 다양한 분야로 활용되고 있다. 향후, 대부분의 디지털 기기에서 Bluetooth 등의 무선 연결을 통한 실시간 상호작용이 일반화될 것으로 예상된다.

그러나 무선 프로토콜은 전파를 매개로 통신이 이루어지기 때문에 물리적 접촉 없이도 다양한 형태의 공격에 노출될수 있다. 실제로 BLE (Bluetooth Low Energy)는 전력 효율성과 사용 편의성을 중시한 설계로 인해 링크 계층, SMP (Security Manager Protocol), GATT (Generic Attribute Profile)등 여러 계층에서 구조적 취약점이 지속적으로 발견되고 있다. 이를 악용한 무선 공격 사례 또한 증가 추세에 있어, 무선 보안 취약점 연구가 필요한 상황이다. 따라서, 본 연구에서는 Bluetooth Low Energy (BLE) 프로토콜의 구조적 취약점을 악용한 여러 종류의 무선 공격을 조사하고 실제 실험 환경에서 적용 가능성을 논의한다.

Ⅱ. 본론

본 장에서는 BLE 프로토콜의 구조와 보안 메커니즘을 기반으로 실제 MITM(Man-in-the-Middle)이 가능한 BLE 프로토콜 관련 공격의 원리를 분석한다. 이를 통해 현재 BLE 보안의 한계와 향후 대응 방향을 논의하고자 한다.

2.1 BtleJuice [1]

BtleJuice는 BLE 프로토콜의 구조적 특성과 보안 취약점을 악용하여 설계된 능동형 MITM 공격의 한 형태로 하나의 BLE 장치는 동시에 두 개의 장치에 연결될 수 없다는 BLE의 연결 제약을 우회하는 방식으로 동작한다. 이 공격은 BLE의 링크 계층에서의 연결 구조, SMP에서의 키 교환 과정의 취약점 그리고 GATT 계층의 인증 부재 속성을 동시에 악용한다. SMP 계층에서는 Just Works 페어링 방식에서 TK(Temporary Key)를 0으로 설정하는 방식의 구조적 취약점을 이용하여 암호화되지 않은 초기 키 교환 시점을 가로채고 GATT 계층에서는 인증 없이 수행 가능한 write 및 notify 요청을 변조하거나 재전송할 수 있다.

이를 위해 공격자는 두 개의 USB 동글을 사용하고, 각각의 동글을 독립된 VM 또는 시스템에 연결하여 하나는 피해자의 BLE 장치에 연결되는 “가짜 앱”, 다른 하나는 피해자의 앱에 연결되는 “가짜 장치” 역할을 수행하도록 설정한다. 두 동글은 Web Socket 프로토콜을 통해 통신하며 이를 통해 BLE 세션 데이터를 실시간으로 중계, 변조, Replay, Hooking을 할 수 있따. BtleJuice는 Kali Linux 기반 환경에서 구동되며, 웹 기반 인터페이스를 통해 공격자는 BLE 통신 흐름을 감시하거나 특정 GATT 특성 값을 조작할 수 있다. BtleJuice는 사용자 기기의 무결성을 침해하거나 모바일 장치를 간접 제어하는데 악용될 수 있다.

2.2 GATTacker [2]

BLE 프로토콜은 GATT를 기반으로 장치 간 데이터를 주고받는 구조를 가지며 많은 장치들이 이 계층에서의 인증 절차를 생략하거나 단순화한다. GATTacker는 이러한 구조적 특성을 악용하는 공격으로 GATT 계층에서 동작한다.

■ Corresponding Authors: Taehoon Kim and Inkyu Bang

공격을 성공적으로 실행하기 위해서는 정상 BLE 장치를 모방한 가짜 장치를 구성하고 피해자의 모바일 애플리케이션이 이를 실제 장치로 오인하여 연결하도록 유도해야 한다. 이 과정에서 공격자는 실제 장치로부터 GATT 서비스와 특성 구조를 복제하고, 읽기, 쓰기, 알림 등의 BLE 이벤트를 조작함으로써 MITM 공격을 수행할 수 있다.

이 공격을 통한 MITM 공격을 진행하기 위해 공격자는 두 개의 BLE 동글(하나는 피해자 앱과 통신, 다른 하나는 실제 장치와 통신), GATTacker 도구, Linux 기반 환경이 필요하다. 이 공격은 BLE 장치 간 데이터 흐름을 중간에서 가로채거나 조작함으로써 사용자 정보의 기밀성 및 무결성을 침해하고 장치 오작동이나 서비스 오용을 유도하는 것을 목적으로 한다.

2.3 InjectaBLE [3]

InjectaBLE은 BLE 프로토콜의 링크 계층 취약점을 악용하여 이미 설정된 연결에 악성 트래픽을 주입하는 공격이다. 이 공격은 윈도우 확장(Window Widening) 메커니즘을 악용하여 프레임 주입 타이밍의 경쟁 조건(Race Condition)을 만들어낸다. 이를 통해 ATT 요청(읽기/쓰기), LL 제어 프레임, CONNECTION UPDATE PDU 등을 삽입함으로써 기능 트리거, 역할 탈취(Master/Slave), 중간자 공격을 수행할 수 있다.

기존 BLE 공격 방식은 대부분 연결 설정 이전 단계에서 수행되며, 재밍(Jamming)이나 광고 패킷 스푸핑 같은 침해적인 기법에 의존하였다. 반면 InjectaBLE은 이미 설정된 BLE 연결 이후에도 공격이 가능하다. 비침해적인 방식으로 기존 통신 흐름을 해치지 않으면서도 악성 프레임을 주입할 수 있다. 즉, 기존 연결을 끊거나 방해하지 않고도, 장치의 기능을 트리거하거나 역할을 탈취하거나 중간자 공격을 수행할 수 있다. InjectaBLE은 BLE 프로토콜 자체의 설계적 허점을 노린다는 점에서 다른 공격과 차별성이 있으며, 기존 BLE 공격과 다르게 보안 위협 범위를 연결 이전에서 연결 이후로까지 확장하였다.

Ⅲ. 결론

BLE는 저전력 무선 통신이라는 장점에도 불구하고 링크 계층, SMP, GATT 계층에서의 구조적 취약점으로 인해 다양한 무선 공격에 노출되어 있다. 본 논문에서는 BtleJuice, GATTacker, Btlejack 등 대표적인 BLE 프로토콜 공격의 원리를 분석하고 링크 계층, SMP, GATT 계층의 보안 취약점을 확인하였다. 본 논문에서 논의한 BLE 공격의 특징은 표 1에 정리되어 있다.

본 논문에서 논의한 BLE 공격 이 외에도 Ubertooth One, nRF Sniffer, Jammer 등의 다양한 공격 방법이 악용된다면 BLE의 기밀성과 가용성까지 위협을 받을 수 있다. BLE의 보안은 대부분 개발자 선택에 따라 필수 요소만 구현되기 때문에 근본적으로 일관된 방어가 어렵다. 만약 BLE 프로토콜을 개선하더라도 기존에 배포된 수많은 기기들이 업데이트 불가하거나 적용에 제약이 있어 현실적인 대응이 쉽지 않다[4]. 이러한 상황에서 AR기기와 같이 실시간 무선 통신에 의존하는 장비는 공유 사칭, 중간자 공격, 데이터 변조에 취약하며 이는 단순한 정보 유출을 넘어 사용자의 안전까지 위협할 수 있다. 따라서 BLE 통신 환경에 보안성 강화를 위한 표준 정비, 대응 체계 마련이 필요하다.

표 1. MITM 공격 도구 주요 특징 비교

항목	BtleJuice	GATTacker	InjectaBLE
장치/환경	Bluetooth USB 동글 2개 (가짜 앱 / 가짜 장치), Kali Linux	Bluetooth USB 동글 2개 (실제 장치 / 피해자 앱), Linux	Bluetooth 스니퍼 또는 타이밍 제어 가능한 커스텀 무선 장비 (동글 1개도 가능)
공격 목적	BLE write 무결성 침해, 사용자 기기 제어, GATT 특성 변조	BLE 세션 가로채기, 정보 유출, 기능 오용	연결된 BLE 장치 제어, 기능 트리거, 역할 탈취, 민감 정보 탈취
공격 계층	Link Layer, SMP, GATT	GATT	Link Layer, ATT
침해 정도	중간자 위치에서 전방위 조작 가능	가짜 장치로 연결 유도 후 데이터 조작	중대한 기능 탈취/역할 조작 가능

ACKNOWLEDGMENT

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. RS-2024-00444170, 6G 개방형 네트워크 환경에서 트러스트 모델 기반 지능형 침해대응 기술 연구 및 국제협력, 50%)과 2025년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2022-0-01068).

참 고 문 헌

[1] T. Melamed, "An active man-in-the-middle attack on Bluetooth smart devices," Safety and Security Studies, vol. 15, 2018.

[2] S. Jasek, "Gattacking Bluetooth smart devices," in Black Hat USA Conference, Las Vegas, NV, USA, Jul. 2016.

[3] R. Cayre, et. al, "InjectaBLE: Injecting malicious traffic into established Bluetooth low energy connections," 2021 DSN, Taipei, Taiwan, 2021, pp. 388-399.

[4] A. Barua, et al., "Security and privacy threats for Bluetooth low energy in IoT and wearable devices: A comprehensive survey," in IEEE Open Journal of the Communications Society, vol. 3, pp. 251-281, 2022.