블루투스 저에너지 재연결에 대한 스푸핑 공격

이전에 연결됐던 장치를 다시 연결하는 매커니즘에 중점!

공격자는 이전에 연결됐던 서버인 척하고 스푸핑된 데이터를 장치에 공급

<일반적인 BLE 통신 절차>

1. 서버(핸드폰 등)은 자신의 신원을 포함한 광고 패킷을 방송하여 존재를 나타냄
2. 클라이언트는 광고 패킷을 스캔해 서버와 무선 연결을 설정
3. (선택적) 클라&서버 간 페어링하여 장기 암호화 키 공유. 데이터를 암호화하고 인증하기 위해 사용
4. 클라가 서버의 데이터에 접근하기 위한 요청 보냄
5. 서버는 클라의 접근 권한 확인 후 읽기/쓰기 권한 부여

서버의 데이터는 속성(혈압, 심박수, 걸음수 등)으로 정리됨. 서버는 각 속성에 대한 접근 제어 정책 지정 가능. 보안 정책은 4단계로 1. 보안 없음 2. 암호화만 있음 3. 암호화 및 인증 4. 인증을 통한 강력한 암호화

<실험 환경 가정>

공격자는 서버, 클라 간 메시지 도청, 수정, 가로채기 가능. 통신 채널에 메시지 주입 가능. 서버와 클라 간 공유 키 모르며 사용된 암호화 기능이 안전함. 공격자, 서버, 클라 모두 블루투스 범위 내 존재

➔ 공격자가 서버를 사칭하여 클라에게 스푸핑된 메시지 전송

Proverif: 재연결 시 인증 프로세스 제공 도구

취약점 1. 선택적 인증: 기본 속성은 암호화 없이도 접근 가능

취약점 2. 인증 우회 가능: 재연결 시

1) 반응형 인증: 클라이언트가 평문의 요청 -> 서버가 보안 수준 불일치 오류메시지 응답 시에만 인증 수행

2) 사전 인증: 클라이언트가 먼저 이전에 공유한 사전 공유 비밀 키를 사용하여 암호화

한 후 인증 수행, 서버가 암호화 활성화하지 못할 시 연결 중단

-> 일부 기기는 사전 인증 실패해도 연결을 끊지 않음!!

BLE Spoofing Attack

- 공격자는 이전에 페어링된 서버의 MAC주소, 광고 패킷 복제
- 클라가 서버로 인식하면 가짜 데이터 제공

반응형 인증 대상: 서버의 오류 응답 x -> 클라가 인증 없이 데이터 수신

사전 인증 대상: 인증 실패 시에도 연결은 끊지 않는 운영체제(특히 Android, iOS)를 이용해 평문으로 데이터 주입

Device Name	**Support for link-layer authentication**
Nest Protect Smoke Detector	×
Nest Cam Indoor Camera	×
SensorPush Temperature Sensor	×
Tahmo Tempi Temperature Sensor	×
August Smart Lock	×
Eve Door&Window Sensor	×
Eve Button Remote Control	×
Eve Energy Socket	×
Ilumi Smart Light Bulb	×
Polar H7 Heart Rate Sensor	×
Fitbit Versa Smartwatch	√
Oura Smart Ring	√

대부분의 실제 BLE 장치는 링크 계층 인증을 사용하지 않음

실제 적용 -> our ring 배터리 상태를 0%으로 위조하거나 '충전 완료' 메시지 위조 등 가능

관련 생각해본 주제...

정상 BLE 연결 vs BLESA 공격을 위한 연결에서의 차이점을 포렌식 로그 등에서 비교해서 미리 이상 징후 잡아내기..?