

예비 지식

BLE (Bluetooth Low Energy)



- Bluetooth 4.0 이후 버전
- 매우 적은 전력으로 무선 통신 가능
- 최근 많은 IoT 기기의 통신 프로토콜로 채택

Beacon

- BLE의 Advertising Packet을 방송하는 장치

Advertising Packet (Beacon Message)

- BLE 기기가 사용자와 연결을 위해 방송하는 신호

IPS (Indoor Positioning System) using BLE

- 실내 위치 측위 : Advertising Packet의 Received Signal Strength Indicator (RSSI) 활용

IPS (Indoor Positioning System) Use Case



Navigation



Rescue



Security



Monitoring

프로젝트 배경

Characteristics of Beacon

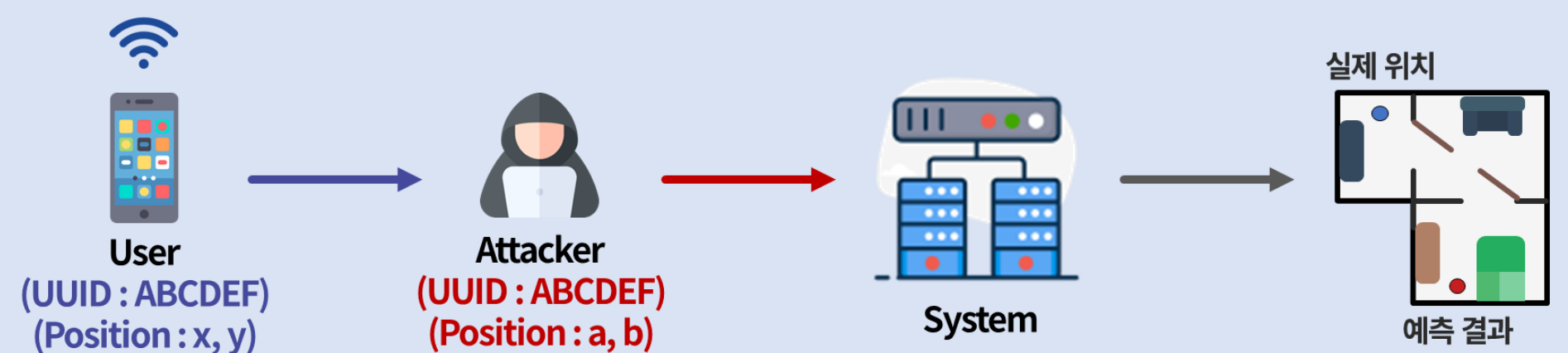
- 공개적으로 Advertising Packet 방송
- 주변 Advertising Packet 확인 및 수집 용이 (E.g., Bluetooth Library (API), App)

Vulnerability of Beacon

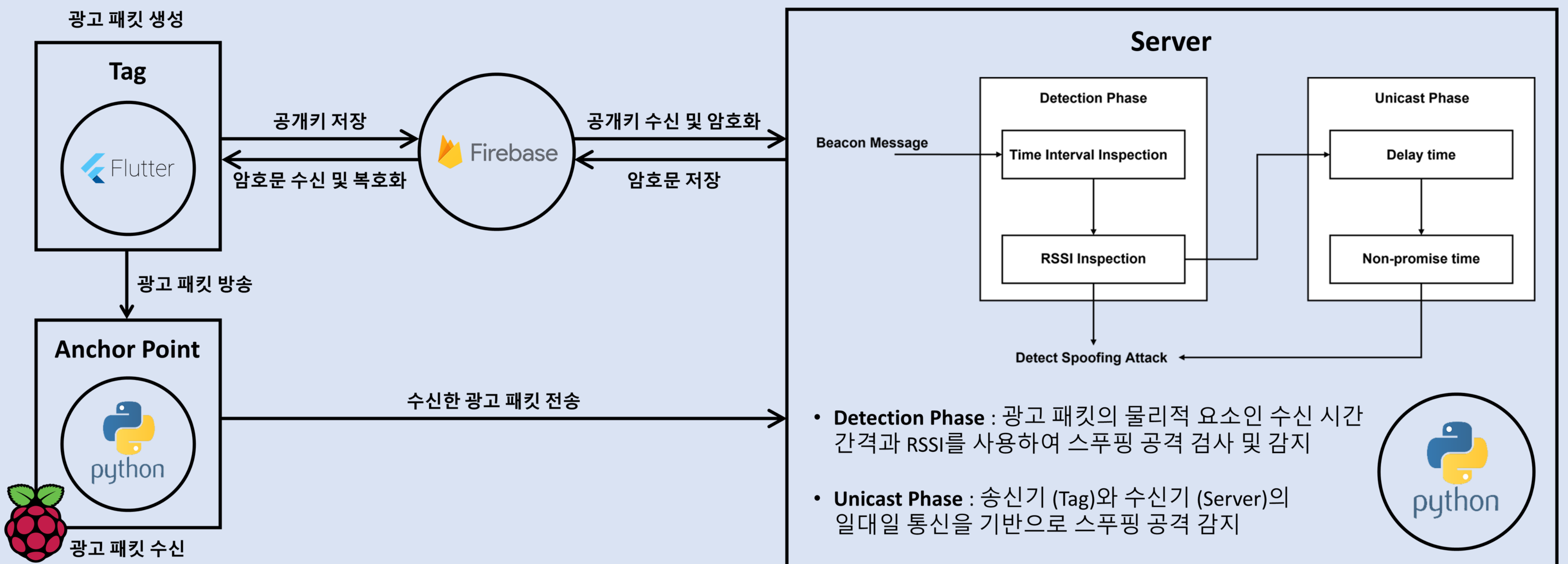
- **Advertising Packet** : BLE 기기의 고유 식별자 정보 포함 (E.g., UUID, MAC Address)
- **Beacon 특징** : BLE 고유 식별자 정보 노출 가능성 높음

Spoofing Attack

- 공격자는 노출된 고유 식별자를 사용해 우리의 BLE 기기인 것처럼 속여 시스템에 접근
- 이후 잘못된 데이터를 전송하거나 데이터를 갈취



시스템 소개



장점 및 기대효과

Limitations of previous studies

- 제한적인 공격 감지 : BLE 기기와 공격자의 거리가 가까운 경우 스푸핑 공격 감지 불가능
- 2차 피해 발생 : 단순히 스푸핑 공격의 감지만 진행

Expected effect of SADS

- 공격자 위치 파악 : 수집된 공격자의 광고 패킷을 활용
- Beacon을 활용한 모든 시스템에서 활용 가능

Advantages of SADS

- 높은 스푸핑 공격 감지 정확도 (About 94%)
- 거리에 관계없이 모든 경우에서 스푸핑 공격 감지
- 공격자의 광고 패킷을 수집하여 공격자 정보 분석