2025학년도 1학기 SW 캡스톤디자인 경진대회

IoT환경에서 IDS(침입 감지 시스템)을 적용한 MQTT 보안

오픈소스 URL : https://github.com/JBNUcapstone

팀 명 적토성산

지도교수 고광신

팀 원 김준혁(컴퓨터공학부, 4학년), 류하영(IT지능정보공학과, 4학년)
박지원(컴퓨터공학부, 4학년), 조재성(컴퓨터공학부, 4학년)

산업체 (주) 바이오라인

개발 동기 및 목적

최근 IoT(사물인터넷) 환경과 스마트팜, 스마트홈, 스마트팩토리 등 다양한 분야에서 MQTT 프로토콜이 널리 사용되고 있습니다. 그러나 실제 현장에서는 MQTT 서버와 브로커가 기본적인 보안 장치 없이 인터넷에 노출되어 있는 사례가 많으며, 이로 인해 다양한 해킹 사고가 반복적으로 발생하고 있습니다. 지펜테스트(Z-Pentest) 스마트팜 해킹 사건에서는 실제 농장 시스템의 MQTT 통신이 해킹되어, 외부 공격자가 센서 데이터와 제어 명령을 조작하는 피해가 발생했습니다. 전북대학교 해킹 사건에서는 수십만 명의 개인정보가 유출되었고, SKT, YES24 해킹 등에서도 대규모 데이터 유출과 서비스 마비가 이어졌습니다. 실제 해킹 사례들은 MQTT 서버가 보호되지 않으면 IoT 네트워크 전체가 위험해지고, 데이터 유출이나 시스템 통제권 상실, 봇넷 감염 등 심각한 피해로 이어질 수 있음을 보여줍니다. 이처럼 IoT, MQTT 환경의 보안 취약점은 단순한 시스템 장애를 넘어 사회적·산업적 피해로 확산될 수 있기 때문에, 실시간으로 다양한 공격을 탐지·차단할 수 있는 IDS(침입 탐지 시스템) 도입이 필요할 것이라 생각되어 주제를 진행하였습니다.

주요 기술

MQTT 프로토콜
경량 메시징 프로토콜로 발행/구독(Publish/Subscribe) 구조를 사용하여 IoT 센서·기기 간 실시간 데이터 통신을 지원 TCP/IP 기반으로 동작하며 저전력,저대역폭 환경에 최적화

실시간 트래픽 모니터링 및 분석
MQTT 브로커에서 메시지의 토픽, 페이로드, 전송 시각 등 메타데이터를 실시간 수집
트래픽 패턴 분석을 통해 비정상 메시지, 반복 전송, 과도한 요청 등 이상 징후 탐지

이상행위 탐지 알고리즘
DoS(서비스 거부) 탐지, Replay Attack 탐지, Data Injection 탐지, Malformed Size/JSON 탐지,Unauthorized Topic/Subscribe Flood 탐지

데이터 전처리 및 저장
수집된 트래픽 데이터의 정규화 및 저장, 향후 AI 기반 이상탐지, 통계 분석 등에 활용 가능하도록 구조화
다양한 MQTT 브로커 및 IoT 플랫폼과 연동 가능하도록 모듈화 설계지원

개발 내용

트래픽 수집 및 실시간 모니터링 모듈 개발
MQTT 브로커에서 실시간으로 메시지의 토픽, 페이로드, 전송 시각 등 메타데이터를 수집하는 모듈을 개발하였습니다. 수집된 데이터는 각 클라이언트별, 토픽별로 분류·저장되어 실시간 분석에 활용됩니다.

이상행위 탐지 알고리즘 구현
DoS Attack: 1초 내 메시지 전송 횟수가 임계값을 초과하면 즉시 탐지 및 경고.
Replay Attack: 동일 페이로드가 짧은 시간 내 반복 전송될 경우 탐지
Data Injection: JSON 파싱 실패, 필드 누락, 값의 비정상(범위 외/비숫자 등) 여부를 검사하고이상 징후시 경고
Malformed Size/JSON: 비정상적으로 큰 메시지, 파싱 불가 데이터 탐지.
Unauthorized Topic/Subscribe Flood: 허용되지 않은 토픽 접근 및 과도한 구독 요청 탐지
탐지된 이상행위에 대해 관리자에게 실시간 알림을 전송합니다.

결과 및 분석

IDS 시스템 적용 결과
IoT 환경에서 MQTT 프로토콜을 이용한 7가지 주요 공격 시나리오(DoS, Replay, Data Injection, Malformed Size, Unauthorized Topic, Malformed JSON, Subscribe Flood 등)를 실제로 수행하고 개발한 IDS(침입 탐지 시스템)의 탐지성능을 평가하였습니다.
공격 시나리오별 탐지 결과DoS(서비스 거부) 공격: 1초 내 과도한 메시지 전송 시 IDS가 즉시 탐지 및 관리자 경고, 필요 시 연결 차단까지 정상적으로 수행됨.
Replay 공격: 동일 페이로드의 반복 전송이 임계값을 초과할 경우, IDS가 반복 공격을 신속하게 탐지하여 경고
Data Injection: JSON 파싱 실패, 필드 누락, 비정상 값삽입 시 IDS가 모두 탐지하여 관리자에게 알림을 전송함
Malformed Size/JSON: 비정상적으로 큰 메시지, 파싱 불가 데이터에 대해 탐지 및 경고가 정상적으로 발생함
Unauthorized Topic: 허용되지 않은 토픽 접근 시 즉시 탐지
Subscribe Flood: 짧은 시간 내 과도한 구독 요청에 대해 임계값 초과 시 탐지 및 경고가 발생
개발한 IDS 시스템은 MQTT 기반 IoT 환경에서 발생할 수 있는 다양한 공격 시나리오에 대해 실시간, 정확하게 탐지할 수 있음을 실험적으로 입증하였습니다.
스마트팜 산업 IoT 등 실제 현장에 적용 시 보안성 강화와 서비스 안정성, 데이터 신뢰성 향상에 크게 기여할 수 있을 것으로 기대합니다.

전북대학교
SW중심대학사업단