ICS(Industrial Control System) 환경에서의 모니터링 및 악성 트래픽 탐지를 위한 EWS(Engineering Workstation) 전용 프로토콜 구조 분석 시스템

심규석, 구영훈, 이민섭, 김명섭*
고려대학교

{kusuk007, gyh0808, chenlima2, tmskim}@korea.ac.kr

EWS Protocol Structure Analysis System for Traffic Monitoring and Detecting Malicious in ICS Environment

Kyu-Seok Shim, Young-Hoon Goo, Min-Sub Lee, Myung-Sup Kim
Korea Univ.

요 약

산업현장에서는 신속하고, 효율적인 데이터 전송을 위해 상용 프로토콜을 사용하기 보다는 자체적으로 개발된 프로토콜을 사용한다. 이러한 자체 개발 프로토콜은 대부분 보안상의 이유로 프로토콜의 구조 및 스펙을 공개하지 않는다. 그러나 자동화된 산업현장에서 발생하는 모든 명령어를 모니터링하고, 의도적인 악성 트래픽을 탐지하기 위해서는 트래픽 분석은 필수적이다. 정확한 트래픽 분석을 하기 위해서는 해당 기기에서 사용되는 프로토콜의 규격을 분석하는 것이 선행되어야 한다. 기존 비공개 프로토콜 구조 분석하는 방법은 국내, 외에서 많이 소개되었지만, EWS 에서 사용되는 프로토콜을 분석하는 방법은 거의 없다. 본 논문에서는 상용 네트워크 환경과는 다른 ICS 환경에서 발생하는 EWS 전용 프로토콜 구조 분석 시스템을 제안한다.

Ⅰ. 서 론

오늘날 산업현장에서도 네트워크의 활용도가 매우 높아지고 있다. 산업현장 및 기반시설에서 사용되는 EWS (Engineering Workstation)은 표준화된 프로토콜을 사용하지 않고, 독자적으로 개발된 프로토콜을 사용함으로써 트래픽 분석, 트래픽 모니터링 및 보안 강화등의 네트워크 관리 작업이 매우 어렵다. 또한, 독자적으로 개발된 프로토콜은 대부분 보안에 대한 위협 방지등의 이유로 비공개로 되어 있어서 프로토콜의 규격이나 프로토콜을 이용한 트래픽에서 정보를 추출하기 매우 어렵다. 이러한 프로토콜은 대부분 수동으로 분석하게 되는데, 수동적으로 프로토콜의 규격을 추론하였더라도, 여러 환경적 상황에 따라 프로토콜의 규격은 변화할 수 있으므로 자동화된 프로토콜 리버스 엔지니어링 방안이 필요하다.[1,2]

기존 자동화된 프로토콜 리버스 엔지니어링 기술들이 많이 발표되었지만, ICS (Industrial Control System)환경에서 적합한 기술은 아니다. 상용 프로토콜과 다르게 EWS 프로토콜은 트래픽 수집과정에서 다양한 플로우를 발생하는 것이 아닌 한번의 Connection 으로 하나의 플로우를 통해 모든 명령어 및 모든 패킷을 주고받는다. 따라서 하나의 기능을 수행할 때 하나의 플로우를 생성한다. 또한, 기존 자동화된 프로토콜 리버스 엔지니어링 기술 같은 경우 각 메시지 마다 공통된 필드가 존재하지만, EWS 프로토콜의 경우 부분적으로 공개되어 있는 부분을 제외하고는 매 패킷마다 다른 메시지를 전송하기 때문에 기존 방법으로는 EWS 프로토콜의 상세 스펙을 알 수 없다.

따라서 EWS 프로토콜만을 분석할 수 있는 방안이 필요하다. 현재 산업현장에 네트워크 기술이 많이 보급되면서 보안사고가 증가하고 있으며 이러한 사고를 예방하기 위해서는 프로토콜의 구조를 알아야하지만 대부분 비공개로 되어있어 원인분석조차 어려운 상황이다[3]. 따라서 EWS 프로토콜의 스펙을 자동으로 추출함으로써 산업현장을 트래픽만으로 모니터링하고, 악성트래픽을 감지할 수 있다.

본 논문은 본장 서론에 이어, 본론에서 자동 EWS 전용 프로토콜 구조 분석 시스템을 제안하고, 마지막 결론 및 향후연구를 언급함으로써 논문을 마친다.

Ⅱ. 본론

본 절에서는 EWS 수동으로 분석하면서 구조를 파악한 결과를 바탕으로 자동으로 EWS 전용 프로토콜 구조 분석 시스템을 제안한다. 자동 EWS 전용 프로토콜 구조 분석 시스템은 총 5 단계로 이루어진다. 먼저, 트래픽 수집단계, 메시지 정렬단계, 메시지 구조 추론단계, 필드 의미 추론 단계 그리고 마지막으로 세션 분석을 통해 추론된 메시지 구조의 Sequence 를 분석하여, 최종 프로토콜 분석을 마친다.

이 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원과 (No.2018-0-00539-001,블록체인의 트랜잭션 모니터링 및 분석 기술개발) 2018 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF-2018R1D1A1B07045742)

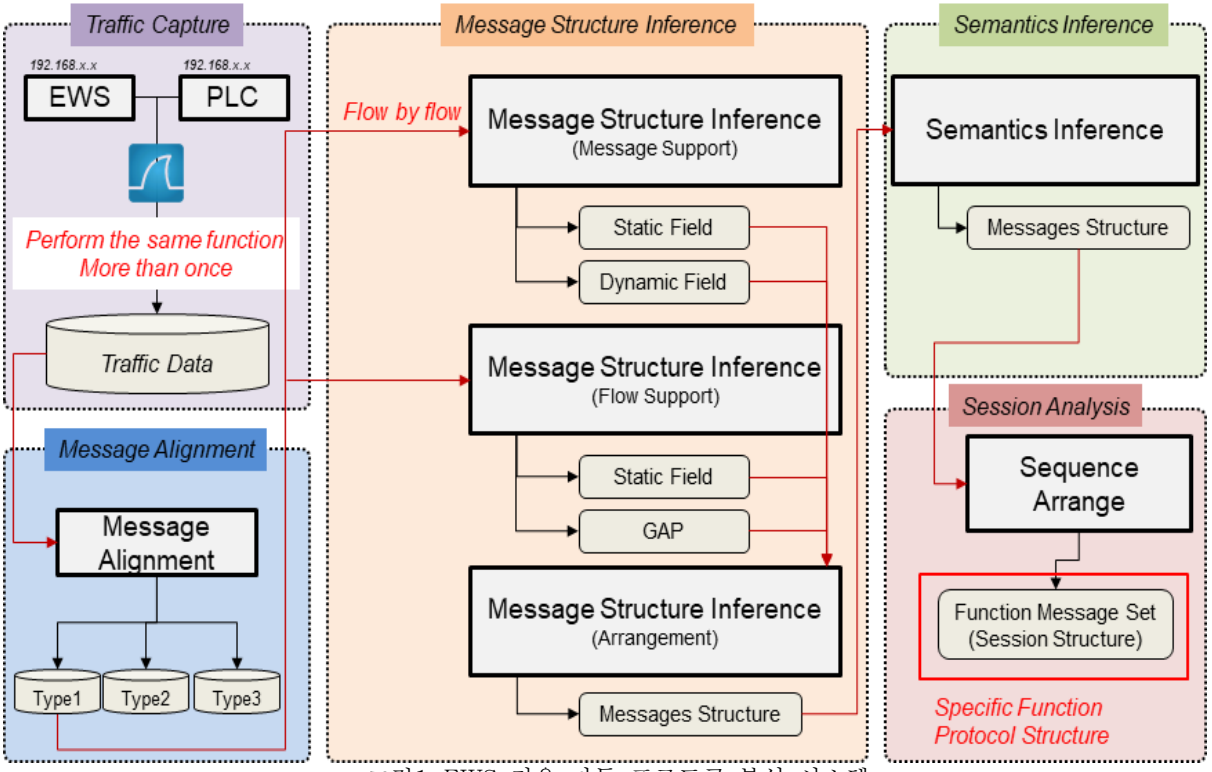

그림1. EWS 전용 자동 프로토콜 분석 시스템

다음 그림 1 은 본 논문에서 제안하는 자동 EWS 전용 프로토콜 구조 분석 시스템이다. 다음과 같이 자동 EWS 전용 프로토콜 분석 방법은 총 5 단계로 나누어진다. 먼저 트래픽 수집단계는 EWS 와 PLC 간에 발생하는 트래픽을 수집하는 과정이다. 본 과정에서 같은 기능을 수행한 트래픽을 두 번 이상 수집한다. EWS 와 PLC 간 연결의 특성상 Connection 한번에 Flow 가 하나만 생성되기 때문에 각 Flow 마다 비교하기 위해서는 두 개 이상의 플로우가 필요하기 때문이다. 두번째는 메시지 정렬단계이다. 메시지 정렬단계에서는 같은 기능을 수행했을 때 비슷한 타입의 메시지별로 정렬을 수행한다. 비슷한 타입의 메시지끼리 정렬시킴으로써 추후 메시지 구조 추론단계를 수월하게 한다.

메시지 정렬단계는 총 4 단계로 구성되어 있다. 먼저 EWS 와 PLC 간의 패킷들 중 Request 와 Response 메시지를 구분한다. 두번째로 각 방향별로 같은 사이즈의 패킷들을 하나의 클러스터로 그룹화하고, 세번째에서 각 같은 클러스터 내에서 다른 패킷들을 분류하기 위해 유사도 측정 알고리즘을 통해 분류한다. 마지막으로 다른 클러스터에서 같은 유형의 패킷을 클러스터하기 위해 유사도 측정 알고리즘을 통해 그룹화함으로써 같은 유형의 메시지를 하나의 클러스터로 그룹화할 수 있다.

메시지 구조 추론단계에서 타입별 메시지의 고정필드, 가변필드, GAP 등을 찾는다. 본 방법론에서는 메시지 구조를 SF(V), DF(V), GAP 으로 정의한다. 네번째 필드 의미 추론 단계에서는 고정필드와 가변필드의 의미를 추론하는 단계이다. 본 과정에서 Seuqence ID, Session ID 을 표현하는 필드를 추출할 수 있다. 마지막으로 세션 분석단계는 메시지의 구조가 추론된 상태에서의 메시지들의 순서를 분석함으로써 어떤 기능을 수행할 때, 어떤 시퀀스의 메시지들이 발생하는지 분석하고, 최종 프로토콜 구조 추론을 완료한다.

Ⅲ. 결론

산업현장 및 기반시설에서 사용되는 EWS (Engineering Workstation)은 표준화된 프로토콜을 사용하지 않고, 대부분 독자적으로 개발된 프로토콜을 사용한다. 독자적으로 개발된 프로토콜은 보안 위협등의 사유로 대부분은 공개하지 않고 있어, 프로토콜의 규격이나 프로토콜을 이용한 제어기기 설정 정보를 추출하기에 매우 어려움이 있다. 따라서 본 연구에서는 EWS에서 사용되는 비공개 프로토콜의 규격이나, 명령어, 설정정보를 파악하기 위해 분석과정에서 자동화할 수 있는 방법을 제안한다.

향후 본 연구에서 제안한 EWS 전용 자동 프로토콜 구조 분석 시스템을 구현하고, 실제 EWS에서 사용되는 프로토콜을 적용함으로써 타당성을 증명한다.

참 고 문 헌

[1] Young-Hoon Goo, Kyu-Seok Shim, Myung-Sup Kim, "Automatic Reverse Engineering Method for Extracting Well-trimmed Protocol Specification," Proc. of the 2018 2nd International Conference on Communication and Network Technology (ICCNT 2018), Stockholm, Sweden, Sep. 22, 2018, pp.1-5.

[2] 구영훈, 심규석, 박지태, 채병민, 문호원, 김 명 섭, "명확한 프로토콜 사양 추출을 위한 프로토콜 리버스 엔지니어링 방법," KNOM Review, Vol. 20, No. 2, Dec. 2017, pp. 11-23.

[3] Denton, G., Karpisek, F., Breitinger, F., & Baggili, I. “Leveraging the SRTP protocol for over-the-network memory acquisition of a GE Fanuc Series 90-30”. Digital Investigation, 22, 2017, S26-S38.