Apriori 알고리즘을 이용한 비공개 프로토콜 구조분석 연구

이민섭, 심규석, 구영훈, 김명섭
고려대학교
{chenlima2, kusuk007, gyh0808, tmskim}@korea.ac.kr

A Study on the Analysis of the Private Protocol Structure using the Apriori Algorithm

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

요 약

오늘날의 네트워크 환경은 매우 급속도로 성장하고 있으며, 이로 인해 인터넷 트래픽이 기하급수적으로 증가하고 있다. 그 결과로 응용 및 악성 행위도 급증하면서 복잡하고 다양한 비공개 프로토콜이 발생하고 있다. 이러한 비공개 프로토콜들의 구조를 분석하기 위해 프로토콜 리버스 엔지니어링 이라는 학문이 꾸준히 연구되어 왔고 이에 대한 중요성은 이미 입증되었다. 기존의 다양한 연구에서 프로토콜 리버스 엔지니어링을 다뤄왔지만 메시지 내에 필드들을 구분하거나 추출하는 표준화된 방법은 존재하지 않기에 본 논문에서는 프로토콜 리버스 엔지니어링에서 메시지 내에 정적 필드들을 정교하게 추출하는 방법을 제안하고 검증한다.

Ⅰ. 서 론

오늘날의 네트워크 환경은 매우 급속도로 성장하고 있으며, 이로 인해 인터넷 트래픽이 기하급수적으로 증가하고 있다. 그 결과로 여러 응용 및 다양한 악성 행위들이 나타나고 있다. 이러한 환경에서 발생하는 복잡하고 다양한 프로토콜들은 보통 알려져 있지 않거나 문서화 되지 않은 비공개 프로토콜 이다. 이러한 비공개 프로토콜의 구조를 분석한다는 것은 프로토콜의 메시지 형식과 의미, 순서 같은 상세한 구조를 추출 하는 것을 목표로 한다. 비공개 프로토콜의 구조를 분석하기 위해서 프로토콜 리버스 엔지니어링 이라는 학문이 꾸준히 연구되어 왔고 이에 대한 중요성은 이미 입증되었다. 프로토콜 리버스 엔지니어링은 네트워크 관리 및 보안 분야에서 필수적인 요소로 자리잡고 있다. 네트워크 관리 분야 에서는 프로토콜 별 네트워크 사용 현황 파악, 한정적인 네트워크 자원들을 효율적으로 사용하고 관리하기 위해 특정 프로토콜에 대한 대역폭 조절 등 네트워크 관리에 활용이 가능하다. 네트워크 보안 분야에서는 네트워크 환경의 급속적인 성장과 더불어 급증하고 있는 여러 악성행위들에 의해 발생하는 비공개 프로토콜들의 구조를 분석함으로써 특정 악성 행위에 대한 정보를 습득하여 대처하거나 기존에 알려져 있지 않은 공격에 대한 탐지 시스템을 구축하는데 활용이 가능하다.

기존의 다양한 연구에서 프로토콜 리버스 엔지니어링을 다뤄왔지만 현재까지 표준화된 필드 구분 및 추출 방법은 존재하지 않으며 각 연구마다 각각의 장단점이 존재한다. 따라서 본 논문에서는 여러 연구들의 장점을 결합하여 프로토콜 리버스 엔지니어링에서의 정교한 정적필드 추출 방법을 제안하고 검증한다.

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No.2015R1D1A3A01018057)과 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2017-0-00513, Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발)

Ⅱ. 본론

1) 프로토콜 리버스 엔지니어링 구성 요소

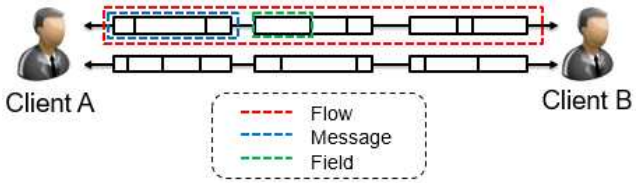

Figure1. 프로토콜 리버스 엔지니어링 구성 요소

본 논문에서 기술하는 필드는 프로토콜 리버스 엔지니어링에서 의미를 가지는 가장 작은 단위를 의미한다. 예를 들어 HTTP 프로토콜의 경우 GET, User-Agent 같은 Method, Header Name같은 것들을 필드라고 정의한다. 메시지는 필드들의 시퀀스로 구성되어 있는데 TCP 플로우의 경우 하나의 TCP 세그먼트, UDP 플로우의 경우 하나의 패킷을 메시지라고 정의한다. 플로우는 5-tuple(Source IP Addr, Destination IP Addr, Source Port, Destination Port, L4 Protocol)이 같은 패킷들의 집합을 의미하며 메시지들의 시퀀스로 구성되어 있다. 본 논문에서는 값이 고정적인 정적필드를 추출하는 방법에 대해 제안하고 검증한다.

2) 정교한 정적필드 추출 방법 제안

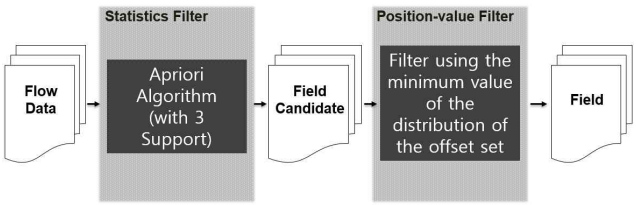

Figure2. 정적필드 추출 방법 Overview

본 논문에서는 필드를 추출하기 위해 두 가지 단계를 정의한다. 첫 번째로 패턴 마이닝의 한 종류인 Apriori 알고리즘에 3 가지 지지도를 적용하는 Statistics Filter 단계, 두 번째로 필드가 메시지 내에서 어떻게 분포하는지를 고려하는 Position-value Filter 단계가 존재한다.

첫 번째로 Statistics Filter 단계에서는 모든 1 바이트 Character를 입력으로 사용하여 Apriori 알고리즘에 3가지 지지도(Message, Flow, Flow Set)을 적용하여 k길이의 빈번한 문자열 집합을 추출한다. Flow Set 이란 하나의 서버와 해당 서버랑 통신하는 클라이언트간에 연결을 맺고있는 모든 플로우들을 원소로 하는 집합을 의미한다. 이 단계를 거쳐 만들어진 k길이의 빈번한 문자열들은 메시지, 플로우, 플로우 집합 모두에서 빈번히 발생하는 문자열이고 필드 후보라고 정의한다.

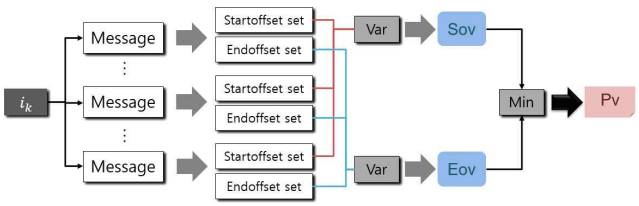

Figure3. Position-value Filter

두 번째로 Position-value Filter 단계에서는 앞 단계에서 추출된 필드 후보들의 분포를 고려한다. Figure3 의 Startoffset set 은 메시지 시작부분을 기준으로 한 필드후보의 위치값들의 집합을 의미하고 Endoffset set 은 메시지 끝부분을 기준으로 한 필드후보의 위치값들의 집합을 의미한다. 특정 필드후보가 나타나는 여러 메시지가 존재하고 메시지 하나당 Startoffset set, Endoffset set 각각 하나씩 존재한다. 특정 필드후보가 나타나는 모든 메시지의 Startoffset set의 모든 원소들의 분산값이 Sov가 되고 Endoffset set의 모든 원소들의 분산값이 Eov가 된다. 이 두 값들중 최솟값을 Pv라고 정의하고 Pv가 특정 Threshold를 만족하면 최종 정적필드로 선택한다.

3) 용어 및 3가지 평가지표 정의

본 논문에서는 비공개 프로토콜을 수집하여 실험하는것은 현실적으로 어렵기 때문에 현재 상용되는 프로토콜 중 하나인 HTTP 프로토콜로 실험을 진행하고 성능을 평가하기 위해 몇가지 용어와 평가지표를 정의한다.

True Field(f) : Method, Version, Header Name, Status Code, Phrase에 해당하는 값
-f_e : True Field중 TFE에 속하는 True Field
-f_n : True Field중 TFN에 속하는 True Field

True Field Format(TF) : 같은 True Field들을 하나로 묶은 것
-TFE : TF중에 EF에 포함되는 TF
-TFN : TF중에 EF에 포함되지 않는 TF

Extracted Field Format(EF) : 추출한 필드
-EFT : EF중 TF가 포함되는 EF
-EFV : EF중 TF가 포함되지 않은 EF

Figure4. 용어

평가지표로는 ConcisenessTF, ConcisenessEF, Correctness 를 정의한다. ConcisenessTF는 TF들 중 TFE의 비율로써 정답지 중에서 어느정도 정답을 추출했는지를 평가하는 지표이다. CorrectnessEF는 EF들 중 EFT의 비율로써 추출한 필드 중 어느정도 정답을 추출했는지 평가하는 지표이다. Correctness는 TrueField중에 TFE에 속하는 TrueField의 비율로써 전체 TrueField들 중에서 어느정도 TrueField를 추출하였는지 평가하는 지표이다.

4) 결과 분석

ConcisenessTF	= 12.98%(10/77)
ConcisenessEF	= 42.30%(11/26)
Correctness	= 42.86%(4850/11315)

Figure5. 실험결과

ConcisenessTF 같은 경우는 77개의 정답지 중에서 10개의 정답을 추출하였다는 것을 알 수 있다. ConcisenessEF 같은 경우는 추출한 필드들 중 약 42%의 정답을 추출하였으며 Correctness는 전체 TrueField 중 약 42%의 TrueField를 추출하였음을 알 수 있다. 결과를 분석해보면 통계적인 정보와 위치적인 정보를 기준으로 추출할 수 있는 정적필드는 추출을 하였으나 빈번하게 발생하지 않거나 위치가 상이하게 나타나는 필드들은 추출이 되지 않았다. 이러한 문제는 지지도들의 Threshold를 낮추면 해결이 되지만 노이즈가 많이 발생하게 되는 문제점이 있다. 따라서 노이즈를 최대한 제거하면서 많은 정적필드들을 추출할 수 있게 하는 최적의 Threshold를 찾는 방법이 필요하다고 판단된다.

Ⅲ. 결론

본 논문에서는 프로토콜 리버스 엔지니어링에서 정교한 정적필드를 추출하는 방법에 대해 제안하고 검증하였다. 통계적인 정보와 위치적인 정보를 활용하여 정적필드들을 추출하였으나 추출되어야 할 필드임에도 불구하고 빈번히 나타나지 않거나 위치가 고정적이지 않은 필드들은 추출하지 못하였다. 따라서 향후 연구로는 노이즈를 최대한 제거하면서 정적필드들을 많이 추출할 수 있게 하는 최적의 Threshold를 찾는 방법에 대해 연구할 계획이다.

참 고 문 헌

[1] 이민섭, 심규석, 구영훈, 김명섭, “프로토콜 리버스 엔지니어링의 정교한 정적필드 추출 방법 제안”, 통신망운용관리 학술대회(KNOM 2018),pp.13-14, 2018년 5월.

[2] 구영훈, Baraka D. Sija, 김명섭, “프로토콜 리버스 엔지니어링의 이상적인 메커니즘 정의”, 통신망운용관리 학술대회(KNOM 2017),pp.23-24, 2017년 6월.

[3] Jian-Zhen Luo and Shun-Zheng Yu, Position-based automatic reverse engineering of network protocols, 2013.

[4] Young-Hoon Goo, Kyu-Seok Shim, Byeong-Min Chae and Myung-Sup Kim, "Framework for Precise Protocol Reverse Engineering Based on Network Traces," Proc. of the NOMS 2018 - IEEE/IFIP AnNet workshop, Taipei, Taiwan, April. 23, 2018.