NetFPGA를 이용한 HTTP Get Flooding 탐지 시스템 개발

황유동*, 유승엽**, 박동규***
*순천향대학교 정보보호학과
**(주)지엔텔
***순천향대학교 정보통신공학과
e-mail:hwangyudong@gmail.com

The Development of HTTP Get Flooding Detection System Using NetFPGA

Yu-Dong Hwang*, Seung-Yeop Yoo**, Dong-Gue Park***
*Dept of Information Security Engineering, SoonChunHyang University
**GNTEL CO. LTD
***Dept of Infomation and communication Engineering, SoonChunHyang University

요 약

본 논문에서는 대용량 네트워크에 비정상적인 트래픽이 유입이 되거나 나가는 경우 패킷 기반의 비정상 트래픽의 탐지와 분석이 가능토록 하는 시스템을 설계하고 구현하였다. 본 논문에서 구현한 시스템은 네트워크상의 이상 행위를 탐지하기 위하여, DDoS HTTP Get Flooding 공격 탐지 알고리즘을 적용하고, NetFPGA를 이용하여 라우터 단에서 패킷을 모니터링하며 공격을 탐지한다. 본 논문에서 구현한 시스템은 Incomplete Get 공격 타입의 Slowloris 봇과, Attack Type-2 공격 타입의 BlackEnergy, Netbot Vip5.4 봇에 높은 탐지율을 보였다.

1. 서론

최근 몇 년 동안 인터넷을 통한 각종 침해사고와 트래픽의 급격하게 증가하고 있으며 이로 인한 피해가 지속적으로 발생하고 있다. 최근의 네트워크 피해사고는 보다 다양화 되고 지능적이며 복합적인 형태로 발생되고 있다. 이러한 네트워크의 비정상적인 상황을 조기에 탐지하기 위한 보다 능동적이고 진보된 기술을 요구된다.[1]

본 논문에서는 통신사업자의 인터넷 백본망에 비정상적인 트래픽의 유입이 되거나 나가는 경우 패킷 기반의 비정상 트래픽의 탐지와 분석이 가능토록 하는 시스템을 설계하고 구현한다.

본 논문에서 구현한 시스템은 네트워크 상의 이상 행위, 특히 DDoS HTTP Get Flooding 공격 탐지 알고리즘을 적용하고, NetFPGA를 통해 라우터 단에서 패킷을 모니터링하며 공격을 탐지한다.

본 논문의 2장에서는 네트워크 상에서 많은 양의 데이터 트래픽을 수집하고 분석하기 위해 사용된 NetFPGA 보드에 대해 소개하고, 3장에서는 본 시스템을 구현하기 위해 적용된 DDoS HTTP Get Flooding 공격 탐지 알고리즘을 설명하고 4장에서는 구현된 시스템에 대해 설명하고 5장에서 결론을 맺는다.

2. NetFPGA[15, 16]

NetFPGA 보드는 IT 기관 및 업체들이 네트워크 대역을 증가시키고 새로운 어플리케이션을 전개하는데 도움을 주며 서버 운용비용을 절감 시켜준다. 보안 측면에서는 고성능, 고효율을 요구하는 어플리케이션 성능을 만족 시킬 수 있는 기능들을 갖춘 고성능 가속 보드로서 네트워크상의 대량의 데이터 트래픽을 검사하여 보안상 위협을 감지하고 그 위협으로 부터의 피해를 미연에 방지하는데 사용될 수 있다.

다음 그림 1은 NetFPGA 하드웨어 구성도이고, 다음 그림 2는 NetFPGA 프레임워크이다.

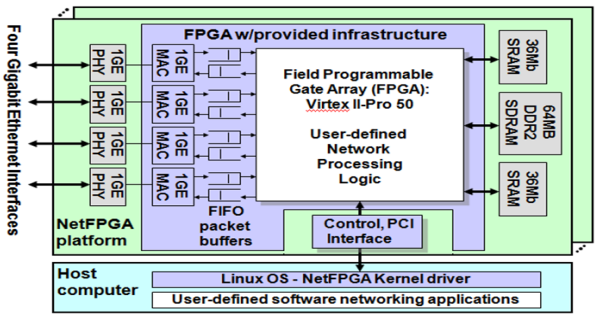

그림 1 NetFPGA 하드웨어 구성도

NetFPA의 주요재원은 다음과 같다.

-Xilinx Virtex-2 Pro FPGA
-Xilinx Spartan FPGA
-2.2.25MB ZBT SRAM
-4*기가비트 Ethernet port
-Linux CentOS 5.2
-듀얼,쿼드코어 CPU

NetFPGA를 이용한 시험환경은 FPGA (Field programmable Gate Array)가 포함된 NetFPGA 카드를 표준 PC에 장착하면 하나의 NetFPGA 시스템이 완성되고, 새로운 설계를 Verilog 코드로 작성하여 FPGA에 로딩 함으로써 쉽고 빠르게 새로운 시스템의 프로토타입을 만들어 낼 수 있다.

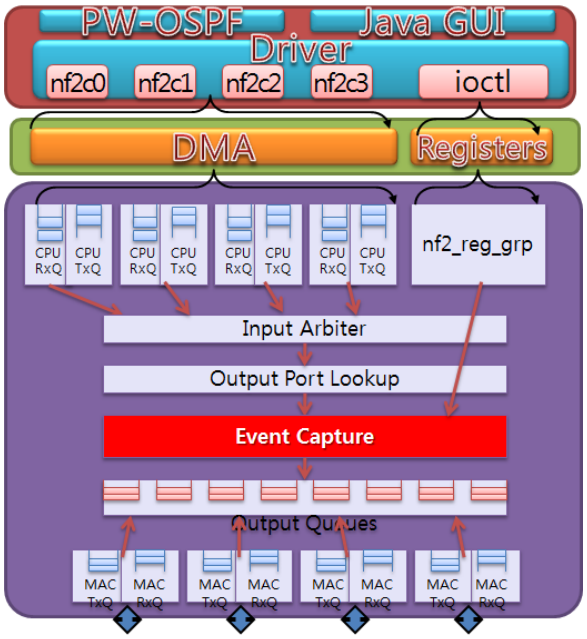

그림 2 NetFPGA 프레임워크

3. DDoS HTTP Get Flooding 공격 탐지 알고리즘 [14]

HTTP Get Flooding 공격의 특성을 분석한 결과 2가지 특성을 얻어냈고, 다음 그림3은 Incomplete Get 연속 특성을 이용한 탐지 알고리즘으로 3 ways hand shake 이후 불완전한 GET or POST가 들어올 경우 ACL테이블의 Get_cnt를 증가하여 임계값이상 들어올 경우 악성패킷으로 판단 한다.

다음 그림 4는 GET flooding 공격에서 사용되는 GET 패킷에는 동일한 URI가 자주 반복되어 사용되는 특성을 이용한 using same URI 탐지 알고리즘이다. IP, Port, URI등을 비교하여 임계값을 초과 하였을 경우 악성패킷으로 본다.

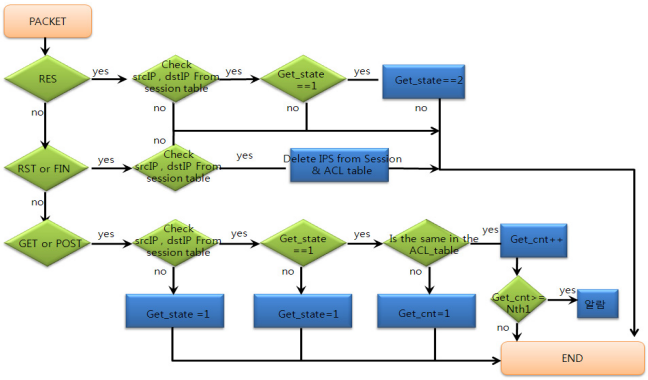

그림 3. Incomplete GET 탐지 알고리즘

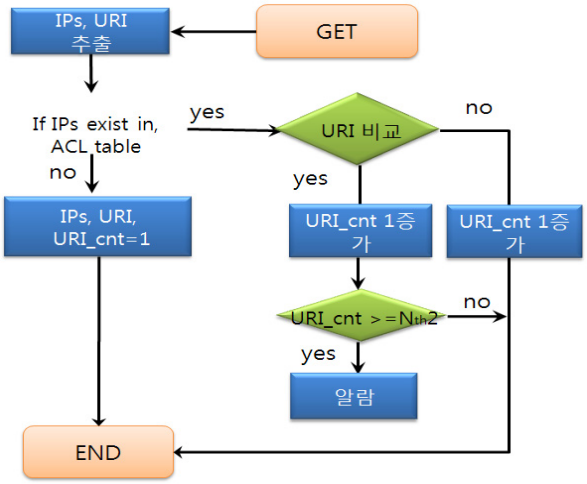

그림 4. GET using Same URI 탐지 알고리즘

4. 트래픽 모니터링 시스템

다음 그림 5는 NetFPGA보드를 통한 트래픽 모니터링 시스템 구성도이다. 그림 5와 같이 네트워크를 링형으로 구성하여 네트워크 상에서 이동하는 패킷을 모니터링한다.

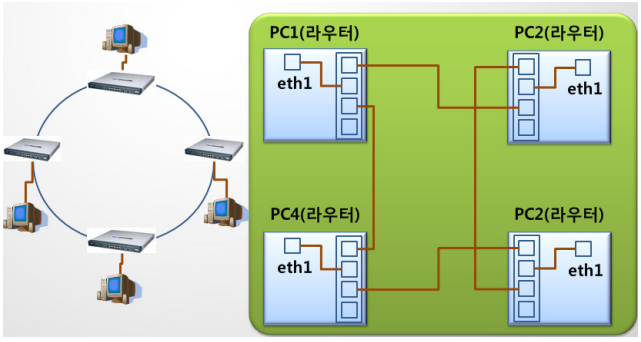

그림 5 시스템 구성도

네트워크에서 NetFPGA보드를 통한 트래픽 모니터링 프로그램 파트의 구성은 아래와 같다.

- 비정상 트래픽 탐지 엔진
- 트래픽 수집 결과를 그래픽으로 보여주는 엔진

다음 그림 6에서 프로그램 파트의 전체적인 처리 흐름을 보여주고 있다. Anomaly 탐지 엔진은 NIC(Network Information Center)로부터 패킷들을 받아와서 정책에 따라 에서 수집된 데이터 트래픽을 수집하고 이상 탐지 알고리즘을 적용하여 얻은 결과 정보를 30초 단위로 그래픽 엔진으로 전달한다. 그래픽 엔진은 전달 받은 결과 정보를 바탕으로 사용자가 보기 쉽게 그램 5와 같이 선형 차트와 히스토그램 그래프 다양한 아스키 리프트를 화면에 그려주고 매 시간 정보 요약 리포트를 생성한다

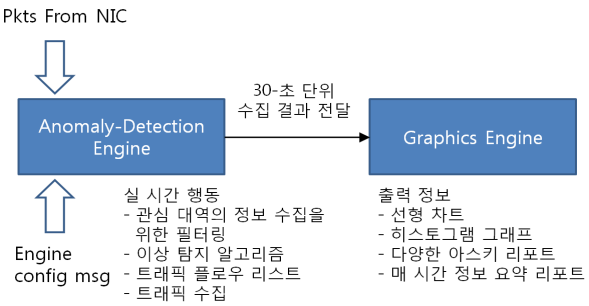

그림 6. 프로그램 파트 시스템 아키텍처

결과적으로 비정상 탐지 알고리즘에 의해 분석된 결과 내용을 그래픽 엔진에 의해 사용자가 쉽게 다양한 결과 정보를 볼 수 있게 된다.

다음 그림 7은 시스템의 각 포트별로 네트워크 패킷의 유입, 유출량을 실시간 차트로 보여주고, 그림 8은 각 포트별 데이터 패킷의 흐름을 로그로 출력한 것이다..

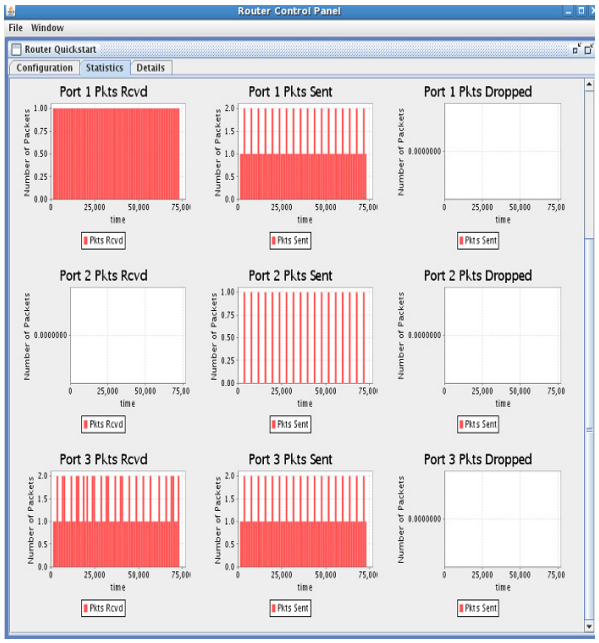

그림 7. 포트별 패킷 유입, 유출량

다음 그림 9는 시스템에서 수집된 네트워크 데이터 패킷을 HTTP Get Flooding 공격 탐지 알고리즘에 적용하여 탐지 결과를 모니터링, 분석하는 프로그램 화면이다.

다음 그림 10은 본 논문에서 구현한 분석 프로그램을 이용하여 봇을 탐지한 결과이다. 시험에 사용된 Slowloris 봇은 공격 타입이 Incomplete Get 이고, BlackEnergy 와 Netbot Vip5.4 는 공격 타입이 Attack Type-2 이다.

그림 8. 포트별 패킷 흐름

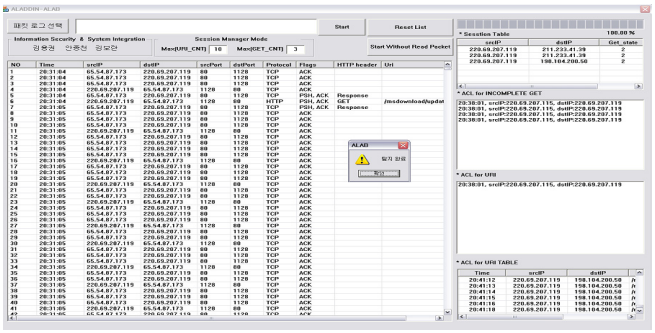

그림 9. 패킷 분석 프로그램

	Incomplete Get 탐지		URI 탐지	
	정탐률	오탐률	정탐률	오탐률
Slowloris	100%	0%	100%	0%
BlackEnergy	0	0	100%	0%
Netbot Vip5.4	0	0	100%	0%

그림 10 탐지율

5. 결론

본 논문에서는 대용량 네트워크에 비정상적인 트래픽이 유입이 되거나 나가는 경우 패킷 기반의 비정상 트래픽의 탐지와 분석이 가능토록 하는 시스템을 설계하고 구현하

였다. 본 논문에서 구현한 시스템은 네트워크상의 이상 행위를 탐지하기 위하여, DDoS HTTP Get Flooding 공격 탐지 알고리즘을 적용하고, NetFPGA를 통해 라우터 단에서 패킷을 모니터링하며 공격을 탐지한다.

본 논문에서 구현한 알고리즘은 몇 개의 악성 행위에 대하여 높은 탐지율을 보였으나, 향후 더 많은 HTTP Get Flooding 공격 툴을 사용하여 구현된 알고리즘의 유효성 검증이 필요할 것으로 사료되고, 탐지 알고리즘에 설정 변수(time, threshold) 들의 최적화가 필요하다. 또한, NetFPGA 보드에 탐지 알고리즘을 내장하여 실제 라우터 단에서 악성행위를 탐지할 수 있도록 하는 연구가 필요한 것으로 사료된다.

참고문헌

[1] Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda§,Xiaoyong Zhou, and XiaoFeng Wang, “Effective and Efficient Malware Detection at the End Host,” usenix security sysposium, 2009.

[2] LI, W, STOLFO, S, STAVROU, A, ANDROULAKI, E, AND KEROMYTIS, A. “A Study of Malcode-Bearing Documents”, In Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2007.

[3] LI, W., WANG, K., STOLFO, S., AND HERZOG, B. “Fileprints: Identifying File Types by N-Gram Analysis” In IEEE Information Assurance Workshop, 2005.

[4] KRUEGEL, C., ROBERTSON, W., AND VIGNA, G. “Detecting Kernel-Level Rootkits Through Binary Analysis“, In Annual Computer Security Applications Conference (ACSAC), 2004.

[5] KINDER, J., KATZENBEISSER, S., SCHALLHART, C., AND VEITH, H. “Detecting Malicious Code by Model Checking” In Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2005.

[6] CHRISTODORESCU, M., JHA, S., SESHIA, S., SONG, D., AND BRYANT, R. “Semantics-Aware Malware Detection”, In IEEE Symposium on Security and Privacy, 2005.

[7] MOSER, A., KRUEGEL, C., AND KIRDA, E. “Limits of Static Analysis for Malware Detection”, In 23rd Annual Computer Security Applications Conference (ACSAC), 2007.

[8] FELT, A., PAUL, N., EVANS, D., AND GURUMURTHI, S. “Disk Level Malware Detection,” In Poster: 15th Usenix Security Symposium, 2006.

[9] KIRDA, E., KRUEGEL, C., BANKS, G., VIGNA, G., AND KEMMERER, R. “Behavior-based Spyware Detection,“ In 15th Usenix Security Symposium, 2006.

[10] YIN, H., SONG, D., EGELE, M., KRUEGEL, C., AND KIRDA, E. “Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis”, In ACM Conference on Computer and Communication Security (CCS), 2007.

[11] Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda§,Xiaoyong Zhou, and XiaoFeng Wang, “Effective and Efficient Malware Detection at the End Host”, usenix security sysposium, 2009.

[12] Yoshiro Fukushima, Akihiro Sakai, Yoshiaki Hori, and Kouichi Sakurai, "Malware Detection Focusing on Behaviors of Process and its Implementation", JWIS, 2009.

[13] “악성 봇의 호스트 전염 특성을 이용한 효과적인 행동기반 탐지기법”, 유승엽, 박동규, 한국정보기술학회, 2010,06

[14] “URI 및 브라우저 행동 패턴의 특성을 이용한 HTTP GET flooding 공격 탐지 알고리즘”, 유승엽, 박동규, 장종수, 한국정보기술학회, 2011.1

[15] "NetFPGA 기반 미래 네트워크 기술 및 응용 연구“, 김종권, 이종원, 권태경, 김종덕, 최선웅, 최훈규, 이규행, 이덕환, 지충섭, 김석환, 안신우, 최영광, 한국정보화진흥원, 2009.12.31

[16] NetFPGA, (http://www.netfpga.org/)