GAM을 이용한 가상 Malware와 실제 Malware의 네트워크 데이터 비교 및 검증

이호섭 이수영 조재익 문종섭

고려대학교, 정보보호연구센터

hslee@cist.korea.ac.kr, {leesuyoung, chojaeik, jsmoon}@korea.ac.kr

Comparing Network Data of Virtual Malware and Real Malware using GAM

Hosub Lee Suyoung Lee Jaeik Cho Jongsub Moon

Center for Information Security Technologies (CIST), Korea University

요약

Malware는 인터넷 혹은 일반 네트워크 사용자의 컴퓨터에 설치되어 의도하지 않은 악의적인 행위와 정보의 유출을 목적으로 하는 프로그램이다. Malware의 성향 분석은 Malware의 행위를 분석하는 것으로서 실제 Malware의 행위를 이용하여 가상의 Malware를 생성하고 두 Malware가 가지는 전파 과정상의 트래픽을 비교함으로써, 네트워크 상의 특성을 비교 및 검증할 수 있다. 본 논문에서는 Malware를 분석하고 가상 Malware를 제작하여 두 Malware가 발생하는 행위, 즉 네트워크 트래픽 데이터를 비교하여 가상의 Malware가 실제의 Malware와 동일한 네트워크 트래픽을 발생 시키는지 확인하기 위해 통계적인 모델링 기법인 GAM 을 이용해 비교 및 검증하는 방법에 대해 제안한다.

1. 서론

통신 기술의 발달은 우리에게 수많은 편의를 주는 반면, 많은 부작용이 뒤따르고 있다. 대표적인 예로 Malware을 들 수 있으며, E-mail, P2P Networks, 인스턴트 메신저, 웹 브라우저 등을 이용하여 자기 복제 및 자가 전파되는 특성을 지닌 인터넷 Malware 가 있다[1]. Malware는 전파방식이 갈수록 다양해지고 지능화되면서 다양한 변종들이 발생하고 있다. 그 이유는 다양한 방법을 통한 self-propagation 이라는 Malware의 전형적인 전파 특성 때문이다. 또한 네트워크 및 호스트들이 고속화 될수록 Malware의 전파속도는 더욱 빨라진다. 한 예로 super worm은 자체 네트워크를 구성할 뿐만 아니라 다른 worm 에 감염된 호스트와 통신을 통해 엄청난 전파속도로 호스트를 감염시킬 수 있다[2].

최근 Malware를 포함한 Malware에 대한 피해가 증가함에 따라, 다양한 관점에서 관련 연구가 진행 중이며, 이러한 Malware를 정형화하거나 분석하여 피해를 예방하고 대책을 세우려는 움직임이 주를 이루고 있다. 미국의 경우, 최근 몇 년 동안 정부와 연구기관에서 Malware에 대한 연구의 중요성을 인식하여, 미국 정부에서 Berkeley 대학에 Malware와 바이러스를 연구하는 테스트베드를 만들어 연구하고 있다[3].

본 논문에서는 실제 Malware와 가상의 Malware가 만들어내는 전파 과정상의 특성을 비교 분석하기 위한 방법으로, 일반화 가법 모형을 이용한 네트워크 트래픽 분석 방법을 제시하고자 한다. 2장에서 기존에 연구된 Malware의 모델링 기법과 통계적 모델링 방법인 일반화 가법모델에 대하여 설명한다. 3장에서는 이 논문에서 두 네트워크 트래픽 데이터를 비교 및 검증하기 위한 방법을 제시하고, 4장에서 제안하는 방법에 대하여 실제 실험 결과를 설명한다. 마지막으로 5장에서 이 논문의 실험에 대하여 결론을 맺는다.

2. 관련 연구

가. Malware 모델링

<표 1> Weaver 가 제안한 Malware 의 분류[5]

FACTOR	TYPE
Target discovery	Pre-generated Target Lists, Externally Generated Target Lists, Internal Target Lists, Passive
Propagation carrier & Distribution mechanism	Self-Carried, Second Channel, Embeded
Activation	Human Activation, Human Activity-Based Activation, Scheduled Process Activation, Self Activation
Payloads	None/nonefunctional, Internet Remote Control, Spam-Relays, HTML-Proxies, Internet DOS, Data Collection, Access for Sale, Data Damage, Physical-world Remote Control, Physical-world DOS, Physical-world Reconnaisance, Physical-world DamageWorm Maintenance
Motivations & Attackers	Experimental Curiosity, Pride & Power, Commercial Advantage, Extortion & Criminal Gain, Random Protest, Political Protest, Terrorism, Cyber Wafare

Malware의 구성요소를 동작방식에 따라 모듈별로 분류한 연구로는 Nazario[4]와 Weaver[5]의 연구내용이 대표적이다.

Nazario 등은 Malware의 일종인 인터넷 worm을 정의하면서 worm의 구조에 대해 reconnaissance capabilities, specific attack capabilities, a command interface, communication capabilities, intelligence capabilities, unused attack capabilities의 6개의 모듈로 분류하면서, worm은 이러한 구성 요소들의 일부 또는 모두를 포함하고 있으며, 보통 여러 형태의 조합을 이룬다고 하였다[4].

Weaver 등은 인터넷 worm이 실행됨에 따라 동작하는 방식을 구조적으로 분석하고, <표 1> 과 같이 worm을 구성하고 있는 요소를 target discovery, propagation carrier & distribution mechanism, activation, payloads, motivation & attacker의 5가지 factor로 분류했다[5]. 이러한 모듈별 분류 방식은 Malware를 구조화하여 인식할 수 있는 기본적인 틀을 제공하였다.

나. 일반화 가법 모형 GAM

일반화 가법 모형 GAM(Generalized Additive Models) 은 지수분포족(정규분포, 이항분포, 감마분포, 포아송 분포, 역 가우스 분포 등)을 따르는 반응 변수 Y에 대한 가법적 비선형 모형으로 1990 년 Hastie 와 Tibshirrani 에 의해 제안되었다[8]. $\mu = E(Y)$ 와 공변량 $X = (X_1, \cdots, X_p)$ 를 연결하는 $\eta = g(\mu)$ 의 형태로

$$\eta(x) = s_0 + \sum_{j=1}^{p} s_j(X_j) \qquad (1)$$

를 계산한다. 여기서 s_0 는 실수이고 $s_1(), \cdots, s_p()$ 는 각각 $x_1, \cdots, x_p$ 의 매끄러운 비선형 함수(smooth nonlinear function) 이며,

$$E[s_j(X_j)] = 0, \quad j = 1, \cdots, p \qquad (2)$$

가 가정된다[6].

3. 제안하는 방법

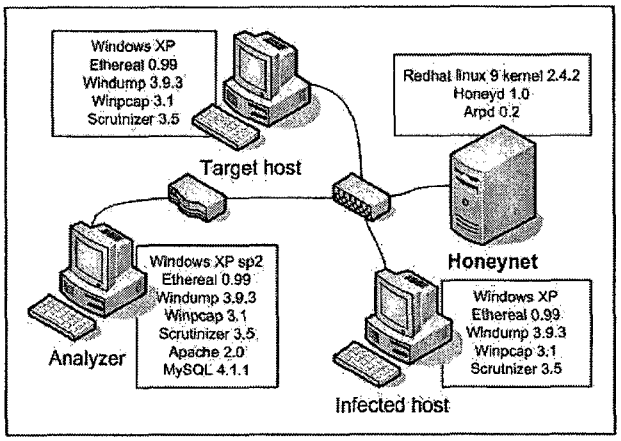
본 논문에서는 위의 Malware 모델링 기법 중 Weaver 가 제안한 방법을 기반으로 실제 Malware 에 대한 네트워크 트래픽 특성을 추출하였다.

추출된 특성을 기반으로 가상의 Malware 를 구현하였으며, 이를 이용하여 실제 Malware 와 가상 Malware 의 네트워크 트래픽을 수집하였다. 또한, 일반화 가법 모형을 통하여, Malware 정형 기법 기반 하에 생성한 가상 Malware 의 네트워크 트래픽과 실제 Malware 의 네트워크 트래픽이 어떠한 형태의 분포 함수를 형성하는지 예측 모델을 생성할 수 있으며, 이러한 특징데이터에 대한 분포 함수가 얼마나 비슷한 형태를 이루는가를 비교함으로써, 가상 Malware 와 실제 Malware 가 같은 특성을 갖는지 검증하는 방법을 제안한다.

가. 네트워크 트래픽 수집

모델링 된 가상 Malware를 실험하는 환경은 <그림 1> 과 같다. 이 실험 환경은 IBM 연구소에서 VMware 를 이용하는 실험 환경을 제안한 기술인 블랙박스 테스트 방식[7]으로 대규모 네트워크에서 나타나는 오버헤드를 줄이기 위해 독립된 네트워크상에서 실제 Malware를 감염시켜 발생하는 트래픽과 모델링된 가상 Malware를 감염시켜 발생하는 트래픽을 비교한다.

본 논문의 실험을 위한 방법은 IBM의 블랙박스 방법을 응용한 것으로서, 라우터 1개와 4개의 호스트로 구성되어 있다. Infected Host 및 Target Host는 패치하지 않은 Windows XP 운영체제를 설치하여 실제 Malware와 가상 Malware를 감염시키기 위한 호스트로 사용되며, Analyzer는 <그림 1> 과 같이 Netflow 클라이언트를 설치하여 네트워크 발생하는 트래픽 데이터를 덤프하여 저장한다. Honeynet은 1개의 가상 라우터와 10개의 가상 호스트로 구성된 가상 네트워크를 구성해 Infected Host가 생성하는 스캐닝 IP 주소의 일부에 대한 응답을 수행한다. Honeynet은 실험 환경으로 독립된 환경을 이용하는 단점을 보완하고 있다.



<그림 1> 네트워크 데이터 수집 환경

나. 주성분 분석을 이용한 입력 데이터 전처리

실험에 사용된 패킷은 ARP, ICMP, TCP, UDP 등 총 4가지이다. 실제 Malware와 가상 Malware를 비교하기 위하여 네트워크 트래픽을 90분간 수집하였으며, 그 중 TCP와 ICMP패킷 데이터가 전체 패킷의 대부분을 이루고 있었다.

<표 2> 시간(분)당 발현 수

TIME	ARP	ICMP	TCP	UDP
1	2	34	226	1
2	0	33	220	0
3	2	34	220	0
4	0	33	220	0
5	0	33	220	0
6	0	33	220	0
7	0	33	220	0
8	2	37	220	0
⋮	⋮	⋮	⋮	⋮

실제 Malware 의 트래픽 데이터와 가상의 Malware 의 트래픽 데

이터의 각 특성이 가지는 성향에 따라, 특성들 간의 차분이 크기 때문에 주성분 분석을 이용하여, <표 2> 의 입력데이터를 센터링 및 표준화 하였다. <표 2> 의 입력 데이터는 수집된 트래픽 데이터로 분당 발현된 프로토콜의 빈도를 계산하여 미리 생성하였다. GAM 을 이용한 각 패킷 데이터의 분포 함수 모델링에는 <표 3> 의 변환된 값을 이용하여 비교 하였다.

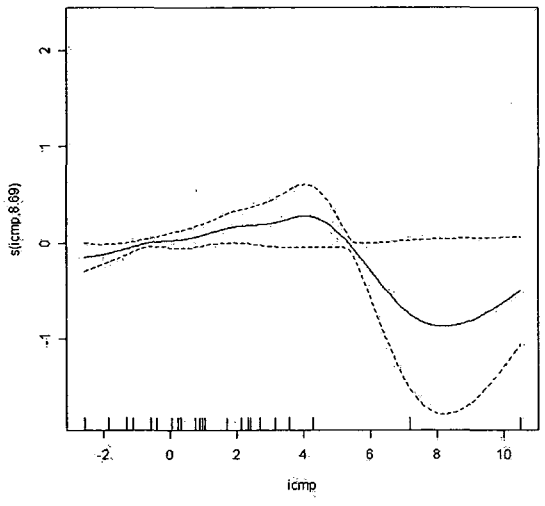
<표 3> 주성분 분석을 이용한 변환 결과

TIME	ARP	ICMP	TCP	UDP
1	-5.59404	0.232564	-1.23257	-0.92684
2	0.509781	-1.1114	0.224117	-0.02398
3	0.326501	0.966338	-0.57708	0.062631
4	0.509781	-1.1114	0.224117	-0.02398
5	0.509781	-1.1114	0.224117	-0.02398
6	0.509781	-1.1114	0.224117	-0.02398
7	0.509781	-1.1114	0.224117	-0.02398
8	-0.19412	3.129432	1.427001	0.246073
⋮	⋮	⋮	⋮	⋮

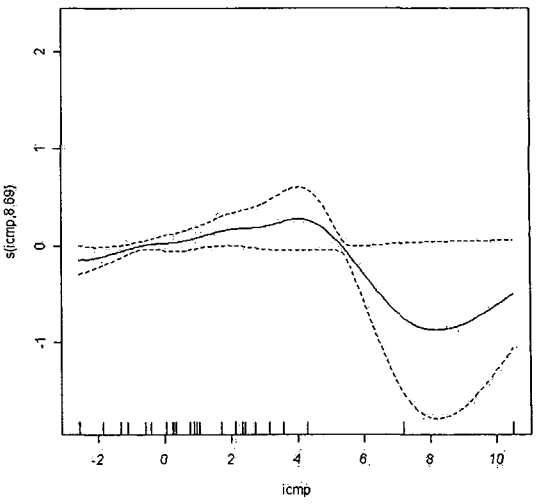
4. 실험 결과

트래픽 데이터를 관측되는 시간에 따른 발현 수를 관측 데이터로 보고 시간에 대한 일반화가법모형을 확인해 보면 그 중 가장 변화량이 큰 데이터인 ICMP 의 결과는 <그림 2>, <그림 3> 과 같다. 또한 전체 트래픽 데이터 중 가장 많은 비중을 차지하는 TCP 의 결과는 <그림 4> 와 <그림 5> 에 나타나 있다.

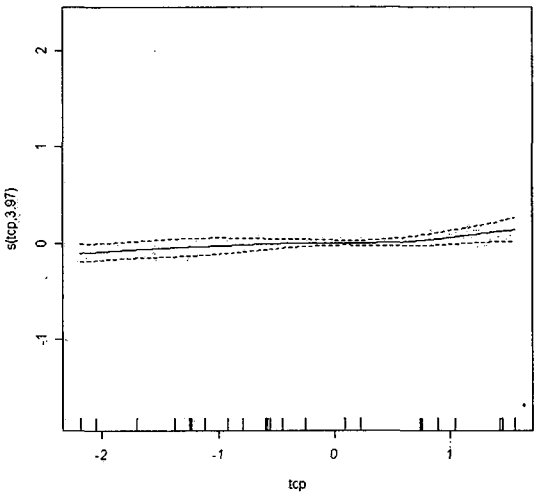
ICMP 를 포함한 모든 데이터를 비교 하였을 때에 GAM은 오류 분포(점선) 이내에서 흡사하였으며, 이로서 가상 Malware의 행위와 실제 Malware의 행위가 동일하다고 확인하였다.



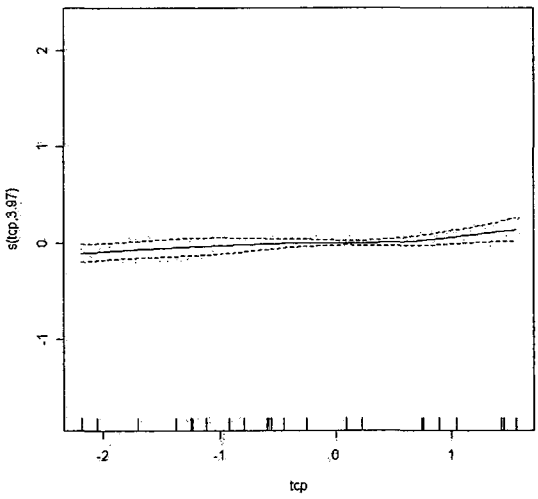
<그림 2> 실제 Malware 의 ICMP 패킷 모델링 결과



<그림 3> 가상 Malware 의 ICMP 패킷 모델링 결과



<그림 4> 실제 Malware 의 TCP 패킷 모델링 결과



<그림 5> 가상 Malware 의 TCP 패킷 모델링 결과

5. 결론

본 논문을 통해, Malware의 동적 분석된 데이터를 기준으로 실제 Malware의 특성에 기반한 전파 방식을 일반화하고, Malware의 전파 과정을 모델링하여, 가상의 Malware과 실제의 Malware을 동일한 네트워크 환경에서 실험하여 비교해 보았다. self-propagation Malware의 전파방식은 대상 호스트를 찾아내어 접속하고, 취약점 공격 코드를 전송하며, Malware 코드를 전송하는 과정을 각각 또는 조합하여 나타낼 수 있고, 이러한 과정을 통해 Malware이 가지는 특성에 따르는 트래픽이 발생하게 된다. 독립된 네트워크에서 전파 방식에 따라 시뮬레이션한 결과를 실제 Malware이 만든 트래픽을 비교 분석했을 때, 실제 Malware과 가상 Malware이 전파 과정에서 발생되는 트래픽의 통계적인 특성이 유사함을 알 수 있다.

이러한 결과는 다양한 Malware의 특성을 조합하여 실험함으로써 해당 Malware의 스캔 비율, 트래픽의 패턴을 예상하고 Malware 전파에 따른 피해나 파급 효과를 예측하는 기본 자료로 활용할 수 있으며, Malware의 전파 특성을 파악할 수 있는 시뮬레이션 환경뿐만 아니라 실제 Malware이 가지는 공격코드가 삽입되어 IDS나 방화벽에 대한 스트레스 테스트 등에 활용이 가능하다.

참고문헌

1. Larry W., Superworm set to attack global e-mails, (2004), http://www.globalcontinuity.com/current_headlines/superworm_set_to_attack_global_e_mails
2. Charles R., ready, set, too late : superworms, (2005), http://news.zdnet.com/html/z/wb/5718933.html
3. Yang S. and Relations M., NSF awards $5.46 million to UC Berkeley and USC to build testbed for cyber war games, (2006), http://www.berkeley.edu/news/media/releases/2003/10/15_testbed.shtml
4. Nazario J., Anderson J., Wash R. and Connelly C., The Future of Internet Worms 2001 Blackhat Briefings, LasVegas, NV, (2001), 4-7
5. Weaver N., Paxson V., Staniford S. and Cunningham R., A taxonomy of computer worms, in Proceeding of the 2003 ACM workshop on Rapid Malcode, (2003), 11-18
6. Trevor H., Robert T., Generalized Additive Models, Statistical Science, Vol. 1 (1986), 297-310
7. Peter Szor, The Art of Computer Virus Research and Defence, Addison-Wesley, (2005)
8. SAS, Generalized Additive Models, http://support.sas.com/rnd/app/da/new/dagam.html