W-TMS(Wireless-Threat Management System)에서의 효율적 관리를 위한 위협 분류기법에 관한 연구

A Study Threat Classification Schemes for Effective Management based on W-TMS(Wireless-Threat Management System)

서종원, 조제경, 이형우
한신대학교

Seo Jong-Won, Jo Je-Gyeong, Lee Hyung-Woo
Hanshin Univ.

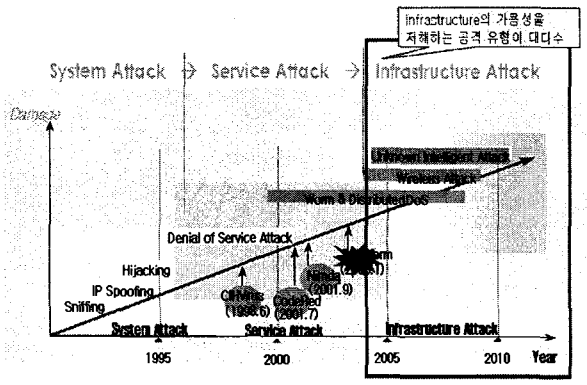
요약

지난 10년 동안 인터넷은 빠른 속도로 모든 분야에 확산되어 왔으면 이와 비슷한 현상으로 최근 몇 년 동안 무선 네트워크의 확산 역시 빠른 속도로 보급되고 있는 추세이다. 그리고 무선 네트워크 침입의 형태와 기술 또한 시간과 비례하여 그 다양성이 점차 증가되고 있으며 공격 시도 및 침입에 성공하는 공격의 횟수도 증가하고 있다. 기존 무선 보안 시스템인 Wireless-IDS는 사고 대응 계획이 설계되고 기획되지 않으면, 보안성을 거의 제공하지 않는다. 그리고 이벤트를 감시하고 사고에 대응하기 위한 인적 요소 비용이 크게 소요되는 단점을 가지고 있다. 기존의 TMS는 필요에 따라 자동화되고 능동적인 대응 수단을 제공하기도 하지만, 새롭게 생성되는 많은 무선 위협의 경우 사람이 막아야 하는 현실을 고려하고 있다. 그리하여 본 연구에서는 무선 상에서의 위협을 자동적으로 관리하는 Wireless-TMS의 효율적인 관리를 위해 수많은 무선 트래픽 중에 위협을 어떻게 분류할 것인가에 초점을 맞추어 연구를 진행한다.

I. 서 론

네트워크의 발달과 더불어 네트워크 공격 유형의 변화도 빠르게 진행되어지고 있다. 과거에는 단일 기법의 소규모적인 시스템 및 서버에 대한 공격 이였지만, 현재는 대규모의 다양한 형태의 다수의 피해를 발생시키는 공격으로 발전해나가고 있다.

이처럼 자동화되고 강력해지는 무선 공격에 대해 보안대책에도 많은 개선방향이 제시되어야 한다. 기존의 IDS의 단순한 공격의 탐지가 아닌 근본적인 공격의 탐지와 대책이 필요한 시점이다. 본 연구에서는 보안 시스템에 인공지능 기술이 더해 네트워크에서 발생하는 모든 위협을 조기에 파악하여 피해를 최소화함으로써 네트워크 자원을 효율적으로 운영하고 관리 할 수 있게 된다. 지능화된 보안 시스템은 트래픽 량과 흐름의 통계적 특성(Statistical Profiles)및 패턴, 웜 및 DoS 공격 등에 의해 발생하는 일시적인 비정상적 트래픽의 패턴을 탐지가능(Anomaly Detection)하다[1].

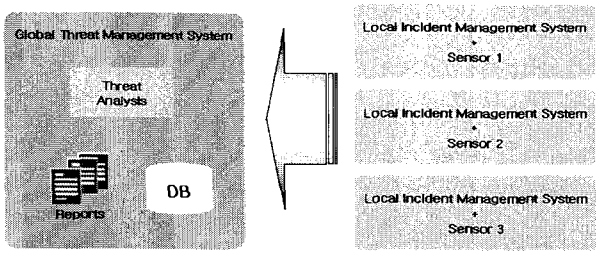


▶▶ 그림 1. 네트워크 공격 유형의 변화

II. 관련연구

1. 기존 TMS(Threat Management System)

위협관리시스템(TMS; Threat Management System)이란 바이러스, 해킹 등 아직 일어나지 않은 사이버 위협을 예측하고 기술과 정보를 상호 보완적으로 결합해 능동적으로 방어할 수 있는 시스템이다. TMS 시스템의 가장 큰 특징으로는 단순히 외부 위협의 통계를 보여주는 것이 아니라 이를 종합적으로 분석해 대응책을 마련할 수 있기 때문에 보다 효과적인 보안 대응이 가능하다는 점이다. 이처럼 네트워크의 위협의 분석을 위해서는 유입되는 패킷에서 위협의 탐지 방법이 가장 중요하다. 이런 관점에서 기존 TMS의 취약점은 위협에 대한 정의가 모호해 전문가의 분석을 통해 객관성이 떨어지는 분석 정보를 시스템 보호 자료로 사용하였다. 그리고 자동화된 위협 탐지가 아닌 분석을 통한 보안 정보를 도출해 내는 방식이므로 실시간으로 유입되는 무선 패킷에 적절한 대응이 어렵다.



▶▶ 그림 2. W-TMS의 핵심 모듈 구조

2. 기존 네트워크 공격 분류 기법

하나의 공격 분류법이 되기 위해서는 충분조건이 되는 항목들이 있다. 이 충분조건들을 많이 수용할수록 좋은 분류법이라 할 수 있다. 그 조건들은 입증성(Accepted[2],[3]), 이해성(Com- prehensible[4]), 완벽성(Completeness [2]-[4]), 확정성(Determinism[5]),상호배제(Mutually exclusive[3],[4]), 반복성(Repeatable [3],[4]), 용어호환(Terminology[4]), 용어선택(Terms well defined[6]), 명확성(Unambiguous [3],[4]), 유용성(Useful[3],[4]) 등이 있다.

Howard의 분류법[3]은 광범위한 공격들을 포함할 수 있는 공격 프로세스 기반(process -based) 분류법이다. 공격자, 도구, 접근, 결과, 목적의 다섯 개의 카테고리로 되어 있다. 공격의 전체 프로세스를 관찰하기에는 적절하지만 구체적인 공격 특성이 나타나 있지 않다. 예를 들면, Code Red와 같은 공격을 이 분류법으로 나누기에는 어려움이 따른다.

Lough의 분류법[7] Lough 는 공격의 특성에 기반을 둔 VERDICT(Validation Exposure Randomness Deallocation Improper Conditions Taxonomy)를 제안하였다. 공격의 특성에 기반하였으므로 새로운 공격이나 혼합형(blended) 공격 등 어떤 공격이든지 분류에 포함시킬 수 있다. 그러나 모든 공격을 포함시키기 위해 분류 자체를 구체적으로 만들지 못했다는 단점이 있다. 예를 들면, 공격에 사용된 구체적인 기법(skill)뿐만 아니라, 이 공격이 흔히 알려져 있는 웜에 속하는지 바이러스에 속하는지에 대한 결정도 모호해진다.

기존의 분류기법들은 너무 일반적인 의미로서만 분류되어 실제 대응 방법 개발에 도움을 받기에는 빈약한 정보를 제공하고, 결국 개발자의 입장에서는 네트워크 보안 시스템이 바이러스, 웜, DoS공격, 스파이웨어(spyware), 애드웨어(adware)등과 같은 수많은 공격들 중 어떤 것들을 차단하려는 목적으로 설계되어야 할 지 조차 불명확해지게 된다[8].

III. 제안 기법

1. 무선 프레임 캡처

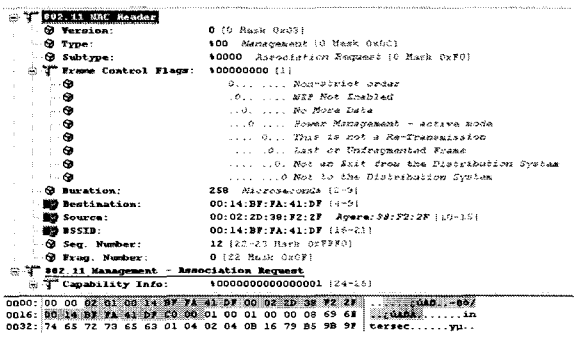
W-TMS(Threat Management System)은 무선 프레임의 캡처에 따라 위협 분석 및 관리의 신뢰도가 결정된다, 즉 무선 프레임의 캡처 없이는 어떠한 위협의 분석 및 관리도 이루어질 수 없다. 그리고 캡처한 데이터를 Global Thread Management System으로 전송해 위협에 대한 탐지 및 분류를 할 수 있다. 이때 무선 네트워크의 Chanel이 존재하는데 이 Chanel Hoping을 통해 모든 Chanel의 무선 프레임을 캡처해야한다.

[표 1] windows 환경에서의 Local Incident Management System 개발 환경

개발 환경	개발 도구	
운영 체제	Windows XP	
개발 언어	C++	
무선랜 카드	무선 랜카드 종류	Atheros Chipset(PCMCIA type)
	디바이스 드라이버	The WildPackets Atheros Wireless Driver v4.2
	지원하는 하드웨어 리스트	http://www.wildpackets.com/support/product_support/airopeek/hardware

2. 좌표공간 위에 무선 프레임 표현

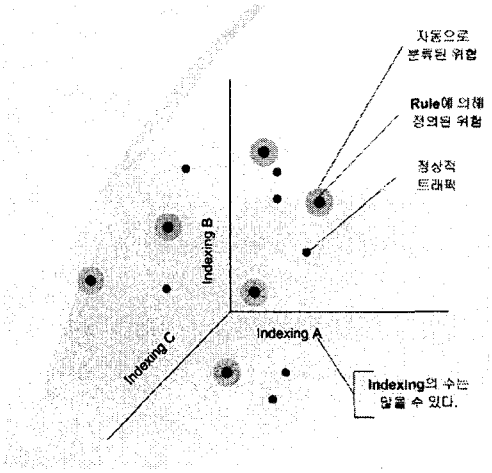
무선 프레임을 좌표 공간에 표현할 경우 위협에 대한 탐지 및 분류가 용이해 진다. 그러나 효율적인 위협의 탐지를 위해 Index 추출(좌표 공간의 축)기준에 따라 위협 분류엔진의 성능이 결정된다. 본 연구에서는 현재 무선 네트워크에 유입되는 무선 패킷들의 헤더 정보를 보고 Indexing된 좌표공간에 표현할 수 있다. 한마디로 이상 트래픽에 대한 탐지를 통해 위협의 추이를 분석하여 앞으로 있을 위협 및 침입에 대한 예상을 할 수 있는 사전감지 시스템을 구축할 수 있다.



▶▶ 그림 3. 무선프레임의 헤더 정보

기존 침입에 대해 좌표 공간에 표현된 위치와 실시간으로 유인되는 무선 프레임 좌표와의 거리를 계산해 위협을 탐지하

고 분류한다. 위협의 탐지 과정 중 임계치 거리의 설정이 위협 분류엔진 성능에 많은 영향을 준다. 본 연구에서는 Index 추출 및 임계치 값(Input 프레임과 기존 침입 프레임과의 거리)에 대한 비교 분석을 통해 보다 지능적이고 최적화된 분류기법을 연구해 안정적이고 자동화된 무선 위협관리 시스템을 구축한다.



▶▶ 그림 4. 좌표공간에 표현된 무선 패킷과 침입 및 위협

3. 위협탐지 방법의 연구

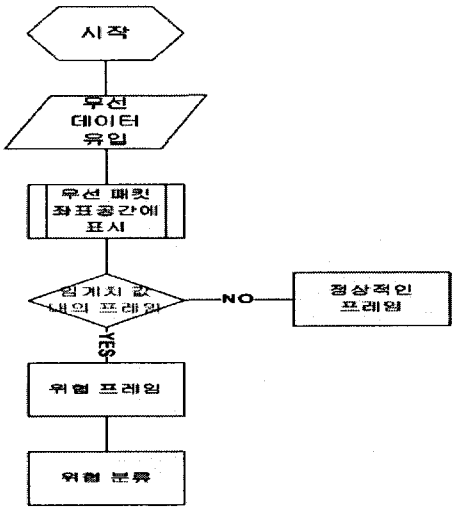
본 연구의 핵심 사항중 하나인 위협의 탐지 방법은 k-NN(k-nearest neighbor) 기법을 이용해 관리자가 설정해 둔 임계치 이하의 거리에 표현되는 Input 프레임은 위협으로 탐지한다. k-NN기법(k-nearest neighbor)이란 분류(classification) 하고자 하는 클래스의 종류에 대해서는 알고 있지만 샘플들 각각에 대한 확률밀도함수 (probability density function) 을 알지 못하는 상태에서 사용한다[9].

$$\bar{d}=\frac{\sum_{i=1}^{N} d_i}{N} \quad (1)$$

수식 (1)[10]의 $\bar{d}$는 최근린(Nearest Neighbour) 거리를 의미한다. [N은 점들의 수를 의미하고, d_i는 점 i의 최근린(Nearest Neighbour) 거리를 의미한다.]

$$E(d_i)=0.5\sqrt{\frac{A}{N}}+(0.0514+\frac{0.041}{\sqrt{N}})\frac{B}{N} \quad (2)$$

수식 (2)의 $E(d_i)$는 Random pattern에서의 최근린 거리의 값 [A는 영역을 의미하고, B는 학습영역 인자의 거리를 의미한다.]

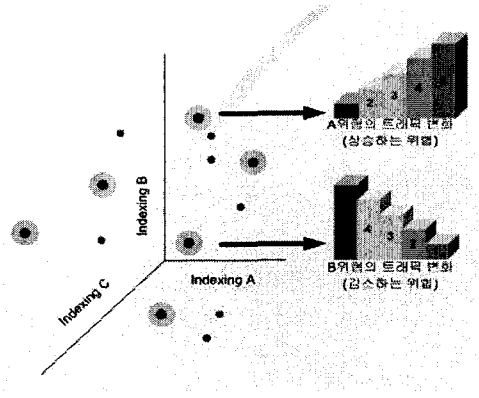


▶▶ 그림 5. 위협 탐지 프로세스

그림 5는 Neural Network의 k-NN(k-nearest neighbor) 기법을 이용한 일반 트래픽에서의 위협의 탐지 과정을 보여주고 있다.

4. 탐지된 위협의 분석 방법연구

분류된 위협은 관리 대상이 되어 분석 대상이 된다. 또 다시 관리의 편의성을 위해 잠재적 위협, 활성화된 위협, 상승하는 위협, 감소하는 위협으로 분류해 단계별로 적적한 대응에 필요한 의사 결정을 지원하기 위해 기술과 정보를 제공한다. (맞춤형 관리 시스템)

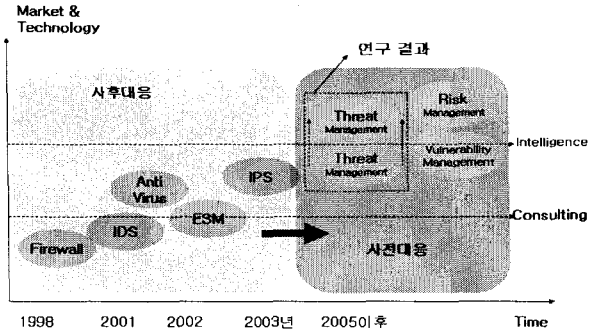


▶▶ 그림 6. 위협 분석 기법

그림 6은 실시간으로 유입되는 무선 프레임의 분석을 통해 위협을 관리 할 수 있는 형태로 변형시킨 것이다. 막대그래프의 값은 유입된 무선 패킷의 수를 의미한다.

IV. 결론 및 향후연구

본 연구는 위협의 단순한 경고 시스템을 넘어 차세대 보안 시스템인 Risk Mangement System에도 활용되어 위험의 실시간 관리가 가능하다. W-TMS와 Neural Network의 k-NN기법을 이용해 정상적인 무선 패킷과 위협 및 공격적인 프레임을 분류할 수 있다. 그러므로 본 연구의 W-TMS는 보다 지능적이고 자동화된 무선 사전경고 시스템이라 말 할 수 있다.



▶▶ 그림 7. 제안 기법의 효과

▌참 고 문 헌▐

[1] 임채호 "능동 보안위협관리" ca expo 2004.

[2] Amoroso E., "Fundamentals of Computer Security Technology," Englewood Cliffs, New Jersey, Prentice Hall, 1994.

[3] Howard J. D., "An Analysis of Security Incidents on The Internet 1989-1995," PhD thesis, Carnegie Mellon University, 1997.

[4] Lindqvist U., Jonsson E., "How to Systematically Classify Computer Security Intrusions," IEEE Security and Privacy, 1997.

[5] Krsul I. V., "Software Vulnerability Analysis," PhD thesis, Purdue University, 1998.

[6] Bishop M., "Vulnerabilities Analysis," International Symposium on Recent Advances in Intrusion Detection, 1999.

[7] Lough D. L., "A Taxonomy of Computer Attacks with Applications to Wireless Networks," PhD thesis, Virginia Polytechnic Institute and State University, 2001.

[8] 김대원, 최양서, 김익균, 오진태, 장종수 "네트워크 보안을 위한 공격 분류법", http://kidbs.itfind.or.kr/WZIN/kugidong/1249/124901.htm

[9] Study Artificial Intelligence "http://www.aistudy.co.kr/pattern /nearest_neighbor.htm"

[10] Richard O.Duda, Peter E.Hart "Pattern Classification and Scene Analysis", WILEY,