외부 해킹 탐지를 위한 사이버 공격 모델링

천양하*

Hacking Detection Mechanism of Cyber Attacks Modeling

Yang-Ha Cheon*

요 약

사이버 침해에 실시간적이고 능동적으로 대응하기 위해 침해탐지시스템(IDS), 침입방지시스템(IPS), 방화벽(Firewall) 등 단위 정보보호시스템 뿐만 아니라 보안장비의 로그, 시스템 로그, 애플리케이션 로그 등 각종 이벤트를 연관, 분석하여 해킹시도를 탐지하는 통합보안관제시스템(ESM)을 사용하고 있다. 하지만 공격이 정교화되고 고도화됨에 따라 기존의 시그니처 기반 탐지 방식의 한계점이 도출되고 있으며, 이를 극복하기 위해 빅데이터 처리 기술을 이용한 공격 모델링에 기반으로 한 징후탐지 기술이 연구되고 있다. 징후탐지 기술의 효과는 공격을 대표하는 특징 점을 정확하게 추출하고, 추출된 특징 정보를 조합하여 실효성 있는 공격 모델링을 수행하는 것이 핵심이다. 본 논문에서는 이와 같은 모델링의 기반이 되는 공격 특징을 추출하고, 시나리오 기반 모델링을 수행하여 지능적 위협을 탐지할 수 있는 방법을 제안한다.

ABSTRACT

In order to actively respond to cyber attacks, not only the security systems such as IDS, IPS, and Firewalls, but also ESM, a system that detects cyber attacks by analyzing various log data, are preferably deployed. However, as the attacks become more elaborate and advanced, existing signature-based detection methods start to face their limitations. In response to that, researches upon symptom detection technology based on attack modeling by employing big-data analysis technology are actively on-going. This symptom detection technology is effective when it can accurately extract features of attacks and manipulate them to successfully execute the attack modeling. We propose the ways to extract attack features which can play a role as the basis of the modeling and detect intelligent threats by carrying out scenario-based modeling.

키워드

Hacking, Modeling, Profiling, Intrusion Detection

해킹, 모델링, 프로파일링, 침입 방지

1. 서 론

오늘날 거의 모든 비즈니스는 컴퓨터와 네트워크에 의해서 이루어지므로 이들에 대한 보안의 중요성이나 날이 증가하고 있다.

수십 년간의 연구와 실제 경험을 가지고 있음에도, 우리는 여전히 안전한 컴퓨터 시스템(Secured Computer System)을 만들어내고 있지 못하고 있으며, 위협의 심각성에 대비한 내부위협 추세 및 행태에 대한 평가와 보안관리에 대한기준이나 연구는 미흡한 실정

* 교신저자(corresponding author) : 용인대학교 (yangha1000@naver.com)

접수일자 : 2013. 07. 23

심사(수정)일자 : 2013. 08. 23

개제확정일자 : 2013. 09. 23

이며, 컴퓨터 시스템의 보안 수준을 정확히 측정조차 하고 있지 못하는 상황이다.[1][2]

이를 해결하기 위해 많은 기관과 기업뿐만 아니라 개인이 운영하는 네트워크 인프라까지도 보안기와 솔루션을 적용하고 각 공격성 접근에 대한 보안등급 적용과 접근제어 기술을 활용하고 있다.[3]

최근 해킹에 대한 대응기술의 발전은 해커들로 하여금 탐지시스템을 우회하기 위한 해킹기술의 변화를 가져오게 만들었으며, 이러한 변화는 APT(Advanced Persistent Threats)로 대표되는 지능적이고 지속적인 공격으로의 변화이다. 지능형 지속위협(APT)은 특정 공격대상의 보안체계의 허점을 이용하여 장기간에 걸쳐 다계층적으로 은밀하게 접근하는 것을 알 수가 있다. 최근에 발생하는 APT공격사례에서도 공격대상은 기술적으로 인지를 하지 못하기 때문에 조직의 지적 재산과 보안과 관련된 정보를 보호하는데 한계가 있을 수밖에 없었다.[4] APT(Advanced Persistent Threats)공격은 2011년도 N기관 전산망 장애, S사 개인정보 유출을 비롯하여 2013년도 3.20 사이버테러와 같은 대규모 해킹사고의 직접적인원인으로 거론되고 있다.

해킹 대응 기술 측면에서는 이와 같은 지능적 공격에 대응하기 위해 관제 측면에서 다양한 분야가 거론되고 있으며, 몇 가지 예시는 빅데이터 처리기술에 기반한 대용량 로그데이터 분석기술[5]과 기존 시그니처 방식의 한계점을 극복하기 위한 증상기반 탐지기술[6]이다.

대용량 로그데이터 분석기술 및 증상기반 탐지기술은 모두 모델링에 기반하고 있다. 이는 현재와 같은 탐지규칙을 시스템에 주입하고 시스템 감사데이터 또는 트래픽 데이터가 탐지규칙과 일치하는 경우 하나의 이벤트로 발생시켜 공격의 가능성을 룰 기반(Rule-based) 탐지기술에서는 제로데이(Zero-Day) 취약점과 장기간에 걸쳐 지속적인 위협을 효과적으로 탐지할 수 없기 때문인 것으로 확인된다.

공격에 대해 보다 효과적으로 대응하기 위한 모델링 기술을 사용하기 위해서는 모델링을 위한 특징정보를 어떻게 추출하느냐와 추출된 특징정보를 어떻게 조합하여 모델링을 수행할 것인가가 관건이라 말할 수 있다. 따라서, 본 논문에서는 모델링을 위한 특징정보를 효과적으로 추출하고 추출된 특징 정보를 이

용하여 프로파일링을 수행하여 APT(Advanced Persistent Threats)와 같은 지능적 공격을 탐지할 수 있는 방법을 제안하고자 한다.

본 논문의 2장에서는 모델링과 관련된 선행 연구를 살펴보고 3장에서는 사이버 공격 탐지를 위한 특징점 추출 방법과 시나리오 모델링을 이용한 탐지 메커니즘을 제안하고 5장에서 결론을 도출한다.

II. 관련 연구

2.1 Petri Net

상태 모델링의 근간이 되는 Petri-Net[7]에 대해 살펴보고, 이를 응용한 상태기반 탐지방법 및 한계점을 분석한다.

Petri Net은 특수한 선도에서 표현되는 동시 병행 시스템의 모델로서, 1960년대에 독일의 C.A.Petri가 고안한 병렬 가동 시스템의 표현법으로 정보 흐름의 표현을 극도로 간소화한 것이다.[7] 이는 프로토콜들을 모델화하는데 주로 사용되며, 장소, 전이, 토큰 등으로 구성되는데, 장소는 0으로, 전이는 -(또는 1)로, 토큰은 ·으로 나타낸다.

그림 1. 페트리 네트에 의한 표현
Fig. 1 Theory according to Petri Net

토큰은 장소로부터 전이를 거쳐서 다른 장소로 움직이며, 이때 통과할 전이는 [Fire]라고 한다. 전이의 각 입력 장소들에 적어도 하나의 입력 토큰이 있으면 그 전이는 활성화(enable)되고 임의의 활성화된 전이는 각 입력 장소로부터 하나의 토큰을 넣음으로써 Fire할 수 있다. Fire할 전이의 선택은 확정적인 것이 아니며, 바로 이 점이 프로토콜을 모델화하는데 유용한 이유가 된다.[8]

2.2 State Transition Analysis

다양한 침입 탐지의 방법 중 상태 전이 분석(State Transition Analysis)[9]은 해커가 시스템 권한을 획득한 후 권한상승을 시도하는 과정 등 해킹의 과정을 시나리오로 만들게 된다. 이 시나리오에는 초기 상태인 compromised state를 포함하고 있다. 상태 전이 분석 방법을 이와 같은 전이 과정에서 나타나는 본질적인 성격 즉, 프로세스 접근, 디렉터리 쓰기 접근 등 다양한 성격을 시나리오로 정의한 다음 이를 기반으로 해킹시도를 탐지한다. 각 전이 단계를 일으키는 해커의 행위를 “Action”으로 정의하였으며, 이 알고리즘에서는 초기 상태나 중간 전이 상태에서 끝나는 Action에 대해서는 무시하고 최종 해킹상태인 Compromised State가 되면 탐지 모듈은 침입이 발생되었다고 경보를 발생해 주는 구조이다.

이 방법에서는 두 가지의 전제조건을 정의한다. 그 첫 번째는 해커는 공격을 위해 파일, 디바이스, 네트워크 통신 등 시스템에 최소한의 권한을 획득하였다는 것이며, 두 번째는 모든 공격을 권한의 획득으로 이어진다는 것이다.

2.3 NetSTAT

상태 전이 분석은 Host 기반의 탐지모델이라 볼 수 있으며, 동일한 구조를 이용한 네트워크 기반의 탐지 모델 NetSTAT 모델[10]이다. 이는 시스템에 침투가 일어나기 전 네트워크에서 발생하는 여러 가지 상태를 시나리오로 정의하여 해킹을 탐지하는 방법이다. 이 모델에서는 감사 데이터(audit data)를 여러 개의 호스트로부터 수집하고 데이터를 조합하여 분석하는 현재의 ESM(Enterprise Security Management) 시스템과 매우 유사한 방법을 사용하고 있다. 대부분의 ESM과의 차이점은 로그를 기반으로 하는 것이 아닌 네트워크의 상태를 기반으로 탐지를 한다는 것이다. 이 외에 NetSTAT 분석 방법을 상태 전이 분석방법과 매우 유사하다.

2.4 한계점 및 개선방향

앞서 살펴본 두 가지의 시나리오 기반 모델링 방법은 Petri-Net을 기반으로 하여 공격으로 발생 가능한 상태를 정의하고 이를 탐지의 기반으로 사용하였다. 이러한 방법을 사용하게 되면 알려진 공격방법을 사

용하여 정확히 일치하는 형태로 공격이 유입되면 정확히 탐지가 가능하나 최근과 같은 다양한 기종의 환경에서 알려진 공격의 변종공격을 능동적으로 탐지하기에는 한계가 있다. 본 논문에서는 이러한 한계점을 극복하기 위해 Check-Point와 Match-Rate 두 가지 개념을 공격 시나리오 모델링에 적용하고자 한다. 즉, 실제 이벤트를 발생시키기 위한 Check-Point를 지점함으로 공격이 처음부터 순차적으로 완벽하게 일치하여 일어나지 않더라도 유사한 공격에 대해 시스템이 이상 증상을 발견할 수 있는 트리거를 생성하고, Match-Rate를 기반으로 알려진 공격 시나리오와 새로이 발견된 이벤트의 유사도를 분석하여 최근 발생되는 지능형 공격을 능동적으로 탐지할 수 있다.

III. 사이버 공격 특징정보 추출 및 모델링

3.1 특징정보 추출

모델링을 위한 사이버 공격 특징 정보를 본 논문에서는 “증상”으로 표현한다. 기존의 물 기반 탐지방법에서는 점검 시점의 리소스 사용량, 패킷의 페이로드 등 “현상”을 기반으로 하였다. 이와 같은 방법을 빠른 비교로 속도의 향상은 가져오지만 시시각각 변화하는 값의 능동적인 반영에는 한계가 있어 결론적으로 오탐을 증가시킨다.

본 논문에서 제안하는 “증상”은 점검 시점의 정적인 상태가 아닌 점검 시점과 시점 간에 변화하는 동적인 상태를 의미한다. 모델링을 위한 특징정보로 사용될 수 있는 상태는 아래 표 1과 같이 정의한다.

표 1. 사이버 공격 특징정보
Table 1. Cyber attack feature

system	Category	Cavalue(Name)	Unit
Server	Resource	Variation	%
	Network	Session State Variation	%
		Session State Count	time
	Log	Category System Log	
		Web logs the number of calls Transition	%
		Web log of Method Transition	%

Firewall	Session	Session Number of Transition	%
		Session Number of Transition	%
Network	BPS/PPS/CPS	Variation	%
		IP Variation	%

이와 같이 시간에 다른 증상의 변화를 특징점으로 사용하는 것은 공격을 보다 정확히 탐지할 수 있는 기반을 제공한다. 즉 일반적으로 정적인 사용량 기반의 탐지조건에서는 자원 사용률이 항상 높은 시스템의 경우 임계점을 정확히 지정하기가 어렵지만 시간에 따른 상태의 변화를 특징점으로 사용하는 이와 같은 방법은 이전 상태 대비 변화하는 기울기를 기반으로 하므로 각 시스템마다 절대적인 수치가 아닌 상대적인 수치를 입력할 수 있도록 함으로 보다 유연한 임계점의 선택을 제공한다.

3.2 사이버공격 모델링

추출된 특징정보를 기반으로 사이버 공격을 모델링하는 방법은 시간과 시간에 따른 시스템별 증상을 표시하는 아래 표 2와 같은 매트릭스 형태로 구성된다.

표 2. 공격 시나리오 모델링
Table 2. Attack scenario modeling

Rule_ID		Step_1	Step_2	Step_n
System_1	Category_1	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_2	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_n	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
System_2	Category_1	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_2	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_n	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
:	:	:	:	:
System_N	Category_1	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_2	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value
	Category_n	Key-name, Key_value	Key-name, Key_value	Key-name, Key_value

Key-name : CA_S의 CAValue 내 Name

Key-value : CA_S의 CAValue 내 Value

이를 수식으로 표현하면 Rule_N은 아래와 같이 모델링 된다.

Rule_n = Step_i(System_id, Category_id,
Key-name, Key-value),
Check-Point, Match-rate

모델링 방법은 먼저 System은 표 1에서 정의한 각 시스템의 아이디를 의미한다. 물의 정의를 위해 먼저 공격시나리오를 분석하여야 한다. 알려진 공격방법을 먼저 분석하여 시간에 따른 시스템과 상태의 조합을 매트릭스로 만드는 것이 일차적인 물이 된다. 물에서 각 Step은 시간의 마일스톤을 의미한다. 한 가지의 증상이 나타나고 다른 증상이 나타날 때 Step이 증가한다. 동일 Step에서는 해킹으로 인해 영향을 받는 별개의 시스템을 포함시킨다. 이와 같은 매트릭스는 2차원으로 보이지만 실체는 3차원의 매트릭스가 된다.

대부분의 알려진 공격은 이와 같은 방법에 의해 탐지될 것이다. 하지만 실제 문제가 되는 것은 이와 같은 알려진 공격이 아니라 변종공격이다. 기본의 시그너처 기반의 탐지방법은 이와 같은 변종 공격을 효과적으로 탐지할 수 없다. 또한 위에서 제안하는 매트릭스도 알려진 공격방법을 모델링한 것이기 때문에 신종 또는 변종 공격에 유연하게 대응할 수 없을 것이다. 이를 극복하기 위해 본 논문에서 제안하는 방식은 Check-Point와 Match-Rate 두 가지 변수를 탐지 물에 사용한다. 알려지지 않은 공격이라 하더라도 공격의 방법이 다를 뿐이지 공격으로 발생하는 증상은 시스템에 부하를 증가시키고 시스템 및 네트워크의 사용량을 증가시킨다. 또한 정보를 유출하는 등 이와 같은 두 가지 변수를 사용하여 기존 알려진 공격과 정확히 일치하지는 않을지라도 부분적으로 일치하는 신, 변종 공격의 발생 가능성을 알려줄 수 있는 기반을 제공한다.

V. 사이버 공격 탐지 메커니즘

3장에서 제안한 동적인 값의 특징정보를 시간의 순서대로 조합한 탐지규칙은 정적인 값을 기본으로 하

는 기존 룰 기반 탐지규칙에 비해 보다 유연하다. 각 탐지 규칙에는 Check-Point와 Match-Rate가 정의된다. Check-Point는 N개의 Step 중 하나로 지정되는데 일반적으로 공격 시나리오상 하위 단계는 상위 단계에 비하여 공격일 가능성이 상대적으로 적으며, 일반적인 증상과 구분이 모호하기 때문에 공격의심으로 판단이 가능한 Step 중 하나를 선정하여 Check-Point로 정의한다. Check-Point는 알람 이벤트 발생을 위한 트리거가 된다. 하나의 증상이 수집될 때 Check-Point와 일치한다면 알람발생을 위한 분석을 시작한다. Match-Rate는 분석 후 알람 발생을 위한 조건이 된다. Check-Point에 해당하는 이벤트가 발생되고 분석결과 수집된 모든 관련 증상이 Match-Rate를 초과한다면 하나의 알람이 발생된다. 이는 알려지지 않은 신종, 변종 공격의 경우도 탐지할 수 있는 기반을 제공하는 본 논문에서 제안하는 핵심적인 요소 중 하나이다. 이 사이버 공격 시나리오 매트릭스를 이용한 탐지 메커니즘은 아래 그림2와 같다.

그림 2. 탐지 메커니즘
Fig. 2 Detection mechanism

탐지 메커니즘의 단계적 절차는 1) 특징정보 수집 2) 특징정보 모델링(룰 생성) 3) 시나리오 매트릭스의 Check-Point와 일치하는 경우 해당 시나리오 추출 4) 해당 시나리오의 각 Step과 수집된 데이터 비교 5) 수집된 데이터와 시나리오의 각 증상과 Match-Rate가 지정된 값 이상이면 알람 발생의 5단계로 이루어진다.

특징정보 수집 단계에서는 네트워크, 시스템, 보안

장비 등의 각종 장비로부터 수집이 가능한 정보 중 해커가 해킹방법을 바꾸더라도 변하지 않는 변화량, 사용량, 접근 리소스 등 증상에 기반한 특징정보를 추출하고 정규화한다. 특징정보 모델링 단계에서는 해킹의 각 단계마다 발생하는 이와 같은 정보를 시간과 장비의 특성에 따라 순서대로 조합하고 이에 대한 임계치를 설정하는 단계이다. 본 메커니즘에서는 이와 같은 모델링 결과를 탐지 룰로 사용한다.

이 방법의 장점은 기존 연구된 방법 대비 공격초기부터 시나리오와 일치하지 않더라도, 공격으로 인해 반드시 영향을 받는 부분을 Check-Point로 정하면 공격자가 다른 유형의 공격 방식을 사용하더라도 탐지가 가능하다는 것이다. 즉 유사 공격을 탐지할 수 있으며, Match-Rate를 정의함으로 기존 시나리오와 100% 일치하지 않는 경우에도 위험징후를 관리자에게 알려줄 수 있다.

VI. 결 론

본 논문에서는 APT(Advanced Persistent Threats)와 같은 지능적이고 알려지지 않은 유사, 변종 공격에 대해 동적인 증상을 기반으로 한 공격 시나리오 모델링 방법을 사용하여 탐지하는 방법을 제안하였다. 본 논문에서 제안한 방식의 핵심은 시나리오 모델링을 위해 동적인 상태의 변화(증상)를 사용한다는 것과 알려진 공격의 유사, 변종 공격도 탐지할 수 있는 유연한 탐지 메커니즘을 구현하기 위해 Check-Point와 Match-Rate의 2개 변수를 사용한다는 것이다. 이로 인해 완벽하게 시나리오가 일치해야만 탐지하여 공격을 막는 기존의 탐지 시스템에서 공격 초기부터 시나리오가 완벽하게 일치하지 않더라도 빠르게 탐지하여 위험한 접근을 차단할 수 있는 탐지 모델링을 제시하였다. 본 논문에서 제안한 방법을 사용하여 현재까지 발생된 사이버 공격 뿐 만 아니라, 향후 발생 가능한 사이버 공격 또한 유연하게 대응이 가능할 것으로 기대된다. 다만, 본 메커니즘을 대용량 엔터프라이즈 네트워크에서 구현하기 위해서는 빅데이터에 대한 처리 기술의 확보가 선행되어야 할 것이다. 향후 본 메커니즘을 적용하기 위한 알려진 공격에 대한 시나리오를 조사, 분석하여 실제 환경에서 적용이 가능하도록 구

현한다면 지능화되고 정교해진 외부 사이버 해킹에 대한 탐지를 쉽게 감지하여 침입에 대한 예방을 할 수 있을 것이다.

감사의 글

본 논문은 2013년도 용인대학교의 지원으로 이루어졌습니다.

참고 문헌

- [1] Dae-kwon Kang, Jeck-chae Euom, Chun-suk Kim, "A Development of Novel Attack Detection Methods using Virtual Honeynet", The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 8, No. 6, pp. 863-872, 2013.
- [2] Cha-in hwan, "A study on the Development of Personnel Security Management for Protection against Insider threat", The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 3, No. 4 pp. 210-219, 2008.
- [3] Woo-Seok Seo, Jae-Pyo Park, Moon-Seog Jun, "A Study on Methodology for Standardized Platform Design to Build Network Security Infrastructure", The Journal of the Korea Institute of Electronic Communication Sciences, Vol. 7, No. 1, pp. 203-211, 2011.
- [4] Yoo-Seok Lim, "Review on the Cyber Attack by Advanced Persistent Threat", Korea Institute of Terrorism, Vol. 6, No. 2, pp. 158-178, 2013.
- [5] McKinsey global Institute, "Big data : The next frontier for innovayion, competition, and productivity", 2011.
- [6] Sang-Yong Choi, Yong-Min Kim, Dea-Jun Joo, Seung-Do Jeong, Bong-Nam Noh, "A Technique of Symptoms Analysis over Time for Detection of APT Attack" SCTA2012, 2012.
- [7] TADAO MURATA, "Petri Nets:Properties, Analysis and Applications" Proceedings of the IEEE, Vol. 77, pp. 541-580, 1989.
- [8] 11"http://terms.naver.com/entry.nhn?docId=832559&cid=209&categoryId=209",Computer Dictionary Compilation Committee, 2011.

- [9] Koral Ilgun, Rechard A. Kemmerer, "State transition analysis: a rule-based intrusion detection approach" Software Engineering, IEEE Transactions on Vol. 21, No. 3, pp. 181-199, 1995.
- [10] Giovanni Vigna, Richard A. Kemmerer, "Net-STAT: A Network-based Intrusion Detection System", Journal of Computer Security, Vol. 7, No. 1, pp. 37-71, 1999.

저자 소개

천양하(Yang-Ha Cheon)

2010년 성균관대학교 대학원 정보통신학과 졸업(공학석사)
2013년~ 숭실대학교 IT정책경영학과 박사과정

용인대학교 교육대학원 전산학 교수

숭실대학교 베어드학부 외래 교수

※ 관심분야 : 모바일 콘텐츠, 빅데이터, 정보보안