Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.507

보안관제 효율성 제고를 위한 실증적 분석 기반 보안이벤트 자동검증 방법*

김 규 일,[1†] 박 학 수,[1] 최 지 연,[1,2] 고 상 준,[1,2] 송 중 석[1,2‡]
[1]한국과학기술정보연구원, [2]과학기술연합대학원대학교

An Auto-Verification Method of Security Events Based on Empirical Analysis for Advanced Security Monitoring and Response;*

Kyu-il Kim,[1†] Hark-soo Park,[1] Ji-yeon Choi,[1,2] Sang-jun Ko,[1,2] Jung-suk Song[1,2‡]
[1]Korea Institute of Science and Technology Information,
[2]Korea University of Science & Technology

요 약

국내 사이버공격 대응 전담조직(CERT)들은 탐지패턴 기반의 보안장비(IDS, TMS 등)를 활용하여 사이버 침해공격에 대한 탐지·대응을 수행하고 있다. 특히, 공공·연구기관의 경우 국가정보원(NIS) 내 국가사이버안전센터(NCSC)를 중심으로 30여개의 부문 보안관제 센터가 구축·운영되고 있으며, 주로 침해위협수집시스템(TMS)을 활용하여 사이버 공격에 대한 탐지·분석·대응을 수행하고 있다. 그러나 현재의 보안관제 체계에서는 대량의 보안이벤트가 보안장비에 의해 발생되고 있을 뿐만 아니라, 보안관제 요원이 보안이벤트에 대한 실제 공격여부를 판단하기 위해서는 추가적인 분석 작업을 수행해야 하므로 보안이벤트 전체에 대한 대응이 현실적으로 불가능한 실정이다. 또한 현재의 보안관제 업무는 보안관제 요원이 보유한 전문지식 및 경험에만 전적으로 의존하고 있기 때문에 특정 보안이벤트에만 분석이 집중되는 업무편중 현상이 발생하며, 이로 인해 기존에 알려지지 않은 새로운 해킹 공격기술에 대한 대응능력이 부족하다. 따라서 본 논문은 실시간 보안관제 및 침해대응 활동의 효율성을 극대화하고 대규모 해킹공격에 대한 조기대응 역량을 강화하기 위해 실제 해킹공격에 대한 실증적 분석에 기반한 대용량 보안이벤트 자동검증 방법을 제안한다.

ABSTRACT

Domestic CERTs are carrying out monitoring and response against cyber attacks using security devices(e.g., IDS, TMS, etc) based on signatures. Particularly, in case of public and research institutes, about 30 security monitoring and response centers are being operated under National Cyber Security Center(NCSC) of National Intelligence Service(NIS). They are mainly using Threat Management System(TMS) for providing security monitoring and response service. Since TMS raises a large amount of security events and most of them are not related to real cyber attacks, security analyst who carries out the security monitoring and response suffers from analyzing all the TMS events and finding out real cyber attacks from them. Also, since the security monitoring and response tasks depend on security analyst's know-how, there is a fatal problem in that they tend to focus on analyzing specific security events, so that it is unable to analyze and respond unknown cyber attacks. Therefore, we propose automated verification method of security events based on their empirical analysis to improve performance of security monitoring and response.

Keywords: Security Monitoring and Response, Automated Verification, Security Events, Empirical Analysis

접수일(2014년 3월 11일), 수정일(2014년 5월 20일), 게재확정일(2014년 5월 21일)
* 본 연구는 2014년도 미래창조과학부의 수탁사업 「과학기술 사이버안전센터 구축 및 운영사업」의 지원을 받아 수행된 연구임(G-14-GM-IR02)
† 주저자, kisados@kisti.re.kr
‡ 교신저자, song@kisti.re.kr(Corresponding author)

I. 서 론

인터넷은 우리나라의 경제·사회 전반을 지탱하는 하나의 중요한 인프라로서 자리 매김하고 있으며, 국민생활에 대한 편리성과 효율성을 제공할 뿐만 아니라 국부 창출에도 지대한 공헌을 하고 있다. 하지만, 인터넷의 발전과 더불어 우리나라는 2003년 「1·25 인터넷대란」을 시작으로 2009년 「7·7 DDoS 공격」, 2011년 「3·4 DDoS 공격」, 2013년 방송·금융사 대상 「3·20 사이버 침해공격」 및 국가기관 홈페이지 대상 「6·25 사이버 해킹공격」에 이르기까지 다양한 형태의 대규모 사이버 공격이 지속적으로 발생하고 있으며, 이로 인해 막대한 양의 경제적·사회적 손실이 발생하였다. 이러한 사이버 위협에 대응하기 위해 국내에서는 「정부 주도형 중앙집중식 보안관제체계」를 도입하고 있다. 이는 국가사이버안전센터(NCSC)를 중심으로 행정, 국방, 금융, 통신, 교육, 과학기술, 보건 등 주요 분야별 특성에 적합한 30여개의 부문 보안관제센터를 구축·운영하고 있으며 Fig.1과 같이 전주기적 정보보호 활동을 위한 관제, 분석, 대응지원의 체계를 갖추고 있다. 과학기술사이버안전센터(S&T-SEC)[7]은 부문보안관제 센터 중 하나로 과학기술 공공·연구기관에 대한 보안관제 서비스를 제공하고 있다.

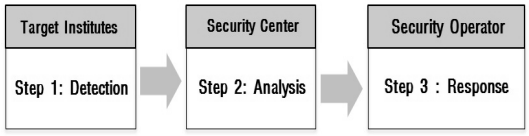


Fig.1. Process for Security Monitoring and Response

이러한 보안관제체계에서는 사이버 해킹공격을 탐지하기 위한 탐지패턴을 공유하고 이를 토대로 신속한 침해공격 탐지·대응을 수행하는 범국가 차원의 일원화된 해킹사고 공조체계 구축에 초점이 맞춰져 있다. 그러나 탐지패턴에 의해 발생된 보안이벤트는 폭발적·지속적으로 증가하고 있으며 보안관제 요원이 해당 보안이벤트에 대한 실제 공격여부를 판단하기 위하여 모든 보안이벤트를 분석하는 것은 현실적으로 불가능한 실정이다. 실제로 보안관제 요원은 1분당 수백~수천건의 보안이벤트를 분석해야하기 때문에 업무효율이 매우 낮다. 또한 현재의 보안관제 업무는 보안관제 요원이 보유한 전문지식 및 경험에만 전적으로 의존하고 있어 특정 보안이벤트에 대한 분석이 집중되는 업무 편중 현상이 발생하며 기존에 알려지지 않은 새로운 해킹 공격기술에 대한 대응능력이 부족하다. 과학기술사이버안전센터(S&T-SEC)의 경우 전체 탐지패턴 중 약 1%만이 실제 보안관제 및 침해대응 업무에 활용되고 있다. 따라서 침해대응 업무에 활용되는 핵심 보안이벤트에 대한 자동분석 및 실시간 검증기술 연구를 통해 실시간 보안관제 및 침해대응 활용의 효율성을 극대화하고 신종·변종 및 대규모 해킹공격에 대한 조기대응 역량을 강화할 필요가 있다.

본 연구는 대용량 보안이벤트에 대한 자동분석을 통해 실제 공격·피해 여부를 신속·정확하게 판단하고 차세대 보안관제 및 침해대응을 수행하기 위한 보안이벤트 자동검증시스템을 제안한다. 자동검증시스템은 Fig.2와 같이 과학기술사이버안전센터에서 탐지된 실제 해킹공격 분석을 통해 사고발생 빈도가 높은 핵심 보안이벤트(상위 20종)를 대상으로 자동검증에 필요한 특징을 추출하고 보안이벤트에 대한 자동검증 시스템을 구축·적용하여 보안관제 업무효율 향상을 목적으로 한다.

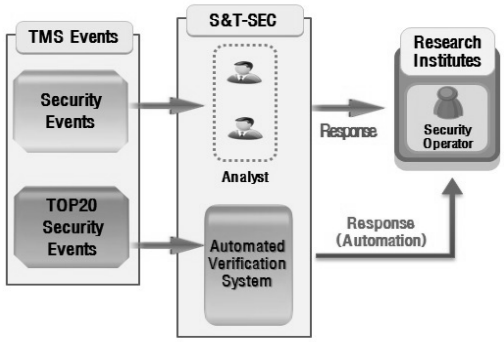


Fig.2. Automated Verification Framework of Security Events

본 논문의 구성은 다음과 같다. 2장에서는 대용량 보안이벤트에 대한 탐지 및 분석업무의 효율성을 높이기 위해 진행되고 있는 침해위협 데이터 간의 집약·제거, 신·변종 공격탐지 및 가시화 기법들을 소개하고 3장은 사고발생 빈도가 높은 핵심보안이벤트에 대한 사고이력 조사 및 자동검증에 필요한 입력정보를 도출한다. 4장에서는 추출된 공통요소를 기반으로 보안이벤트의 특징추출 방법을 제시하고 5장은 자동검증의 시범적용을 위한 시스템 구성 및 설계·구현을 제안하며 6장에서는 제안 시스템의 산출물에 대한 우수성을 제시하고 7장에서는 본 논문의 최종 결론을 맺는다.

II. 관련 연구

본 장에서는 대용량 보안이벤트에 대한 탐지 및 분석 업무의 효율성을 향상시키기 위해 현재 진행되고 있는 보안이벤트 집약·제거, 공격시나리오 탐지방법, 신·변종 공격탐지연구 및 가시화 기법의 기술연구들을 소개한다.

2.1 보안이벤트 집약 및 제거 연구

보안이벤트 집약·제거에 관한 연구는 주로 클러스터링 기술과 유사도 측정기술을 기반으로 한다. 이를 통해 보안이벤트를 동일한 공격으로부터 발생한 집합으로 그룹화하거나 중복된 보안이벤트를 하나의 대표 이벤트로 병합 또는 제거하는 것이 주된 목적이다. 이와 관련하여 Meta-Alarm 개념[1][2]을 이용한 연구가 제안되었으며 보안이벤트를 클러스터링하기 위한 과정은 Fig.3과 같다. AMI (Alarm Management Interface)는 서로 다른 센서로부터 수집된 각각의 보안이벤트를 표준메시지 형태로 변환하는 데이터 정렬기능을 수행한다. Clustering/ Fusion Module는 가장 근접한 이웃 클러스터링 (nearest-neighbour-clustering) 알고리즘[3][4]을 이용하여 분류된 각각의 보안이벤트에 대해 해당 이벤트가 어느 클러스터에 속하는지 결정하게 된다.

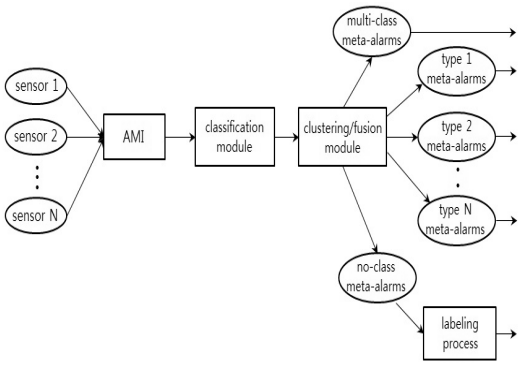


Fig.3. Alarm Clustering Module

2.2 공격 시나리오 탐지에 관한 연구

보안이벤트로부터 공격 시나리오를 탐지하기 위한 연구는 사이버 공격이 단한번의 공격으로 끝나는 것이 아니라, 특정 공격이 최종적으로 성공하기 까지는 여러 단계의 공격과정을 거친다. 따라서 공격과정별로 발생하는 보안이벤트를 하나의 시나리오로 재구성하고 이를 그래프와 같이 보안담당자가 이해하기 쉬운 형태로 표현하는 다수의 연구[8][9][10][11]가 진행되어 왔다. 그 중에서 대표적인 다단계로 이루어지는 사이버 공격을 표현하기 위한 보안이벤트 연관관계 분석 방법이 제안되었으며 Fig.4는 연관관계 그래프를 생성하기 위한 아키텍처를 보여준다. 해당 아키텍처는 먼저 센서에서 탐지된 보안이벤트들이 중앙 데이터베이스에 저장되고 보안이벤트 파서는 저장된 보안이벤트로부터 공격 시나리오를 생성하고 이를 기반으로 관제를 수행하게 된다.

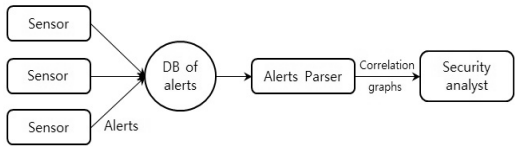


Fig.4. Correlation Graphs Architecture

2.3 신·변종 공격 탐지에 관한 연구

보안이벤트로부터 현재 알려져 있지 않은 신·변종 사이버 공격을 탐지하기 위한 클러스터링 및 일반화된 통계치 추출기법[12][13][14]이 제안되었다.

이들 통계치 기법은 각각의 네트워크 패킷 버퍼로부터 신종 공격을 탐지하기 위해 8개의 통계치를 기반으로 새로운 특징 벡터를 생성한 후 확률기반 분류기(naive bayesian)를 이용하여 네트워크의 이상유무를 판단한다. Fig.5는 네트워크 상태를 판단하는 알고리즘의 프로세스를 나타낸다.

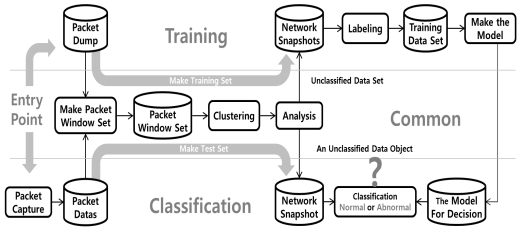


Fig.5. The algorithm for determining the network status

우선, 신종 해킹 공격을 탐지하기 위해 패킷 윈도우로 구성된 버퍼를 생성하고, K-Means 클러스터링을

사용하여 각 패킷 윈도우에 속한 패킷 데이터로부터 특징벡터를 추출한다. 추출된 특징벡터는 네트워크 이상상태를 분류하기 위한 2차 특징벡터를 생성하고 생성된 벡터의 버퍼를 분석하여 공격패킷 구성이 50%이상일 경우, 해당 네트워크 상태를 비정상으로 판단한다.

2.4 침해위협 데이터 가시화 관련 연구

2.4.1 VizAlert 및 VizAware

VizAlert와 VizAware[5]는 Utah 대학에서 개발한 도구로써 IDS 이벤트 간의 상관관계를 가시화하는데 그 목적이 있으며, 이를 위해 IDS 이벤트들의 특징(w3 premise: what, when, where)을 기반으로 시각화하여 전체/개별 관리 도메인의 보안 상황을 인지하도록 하였다. Fig.6은 VizAlert와 VizAware의 가시화 예를 보여준다. VizAlert는 관리 도메인을 중심부에 두고 시간 주기를 의미하는 원들을 중심에서 외부로 그려서 표현하고 있으며, 가장 외부에는 연관성 있는 이벤트의 그룹들을 표현하고 있다. VizAware는 관리 도메인을 토폴로지 정보와 결부시켜 표현하고 있으며 이벤트를 생성한 센서들의 정보를 가장 외부 원상에 표현하여 해당 이벤트의 상세 정보를 제공한다.

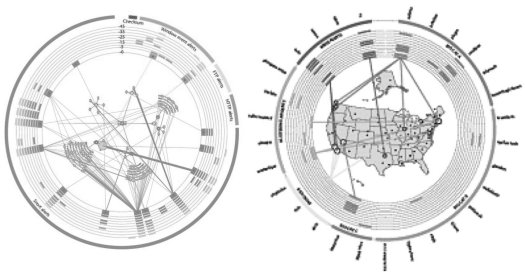


Fig.6. VizAlert(Left) and VizAware(Right)

2.4.2 NVisionIP

NVisionIP[6]는 보안 담당자의 상황인식 능력을 향상시키기 위해 설계되었으며, 전체 네트워크를 감시하는 Galaxy View를 포함하여 세부적인 특정 프로토콜 및 포트를 감시할 수 있는 Small Multiple View, Machine View 등의 Drill-Down 기능을 제공한다. Fig.7은 NVisionIP의 사용자 인터페이스를 나타낸다. NVisionIP는 /16 주소체계(a, b, c, d)의 네트워크(a, b) 부분과 호스트(c, d) 부분을 각각 가로축과 세로축으로 하여 데이터들을 표현하고 있으며 포트들은 특정 색으로 할당하여 가독성을 높였다.

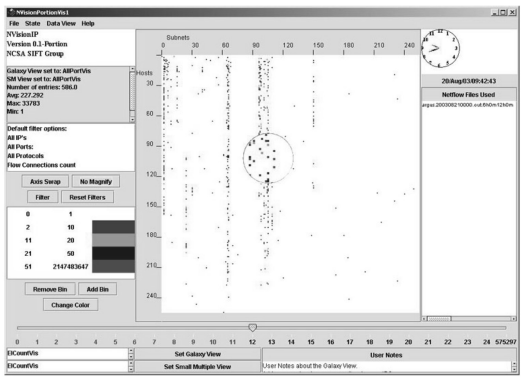


Fig.7. NVisionIP User Interface

III. 자동검증 입력정보 유형 도출

본 연구에서는 수천 개 보안이벤트에 대한 검증요소 및 검증범위를 줄이기 위해 과학기술사이버안전센터(S&T-SEC) 에서 구축·운용 중인 침해위협관리시스템(TMS)을 활용하여 약 7년 3개월간 축적한 실제 사고처리 데이터를 기반으로 자동검증에 필요한 입력정보 유형을 도출하였다. 침해위협관리시스템은 침입탐지시스템(IDS)과 유사하며 탐지 이벤트정보와 패킷분석을 통해 침입시도나 유해트래픽을 탐지하는 시스템이다. Fig.8은 사고발생 빈도가 높은 핵심 보안이벤트에 대한 사고이력 조사 및 실제 악성코드 분석을 통해 자동검증에 필요한 공통요소를 추출하기 위한 프로세스를 보여준다. 우선 2006년 3월부터 2013년 5월까지 과학기술사이버안전센터(S&T-SEC)에서 수집된 TMS 보안이벤트를 분석한 결과, 실제 사고처리건수는 총 12,745건으로 이 중 과학기술사이버안전센터 탐지패턴을 기반으로 한 실제사고 처리건수는 9,036건인 것으로 확인되었다. 우리는 이들 데이터를 활용하여 보안 이벤트를 6개의 침해위협 유형별(웜·바이러스, 자료훼손 및 유출, 홈페이지 위·변조, 경유지 악용, 서비스 거부 및 단순침입시도)로 분류하고 이 중 가장 위험도가 높은 핵심보안이벤트 799종을 선별하였으며 보안을 위해 이벤트 명 중간을 *로 표기하였다. 마지막으로 추출된 핵심보안이벤트에 대한 보안관제 요원의 전문지식, 사고이력 조사·비교, 문헌조사, 유관

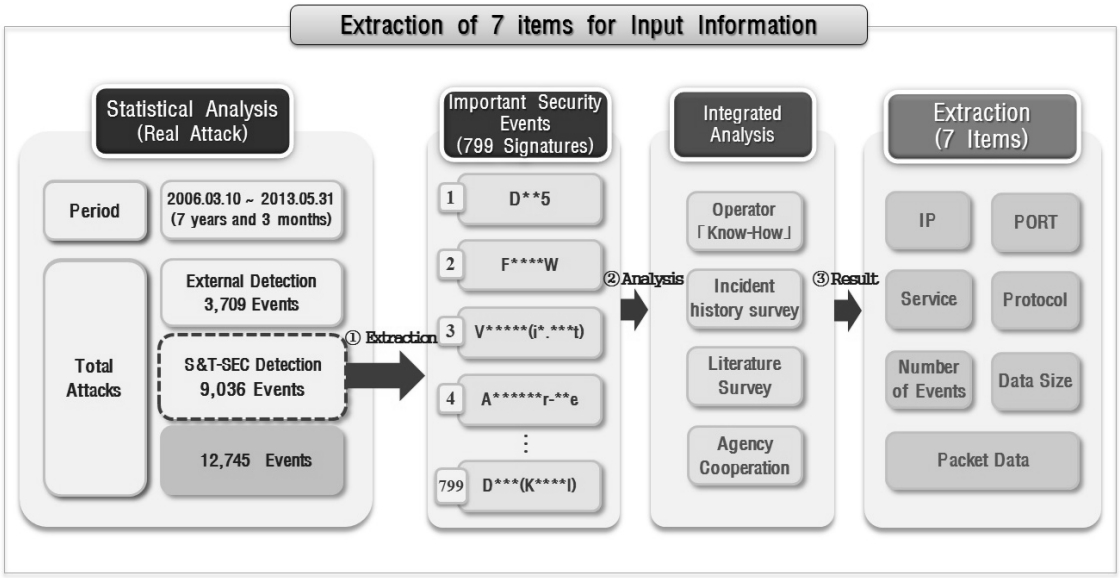


Fig.8. Extraction Process of 7 items for Input Information

기관 협력을 바탕으로 통합분석을 수행하여 총 7개의 자동검증 입력정보를 도출하였다.

자동검증 입력정보 도출결과 Table.1과 같이 7개 입력정보 유형이 도출되었고 이들 유형은 침해위협 전반의 데이터를 기반으로 하기 때문에 각 보안이벤트의 특성에 따라 다소 차이가 발생하지만 자동검증 심층 분석에 필요한 기준을 제시한다.

Table 1. Items of Automated Verification

	Item	Type	Contents
1	IP	String	IP address
2	PORT	Number	Port number
3	Service	String	Network info. (Web server, DNS, etc.)
4	Protocol	String	Protocol info. (TCP, UDP, ICMP)
5	Number of Events	Number	Number of security events
6	Data Size	Number	Data size of security events
7	Packet	HEX	Raw data of security events

IV. 보안이벤트 특징추출

4.1 보안이벤트 특징추출 개요

보안이벤트에 대한 실시간 자동검증을 수행하고 이로부터 해당 보안이벤트에 대한 정·오탐 분류를 수행하기 위해 3장에서 도출한 7개의 자동검증 공통 요소를 토대로 실제 해킹공격의 발생빈도가 높은 문자열 기반의 상위 20종 보안이벤트를 선별하였다. 해당 보안이벤트 특징은 Table.2와 같으며 3장에서 언급하였듯이 보안을 위해 본 논문의 이벤트 명은 중간을 *로 표기하여 기술하였다. 이들 이벤트의 공통점은 웜·바이러스에 감염된 시스템이 경유지 또는 지령서버로 시스템 정보를 전송한다는 점이다.

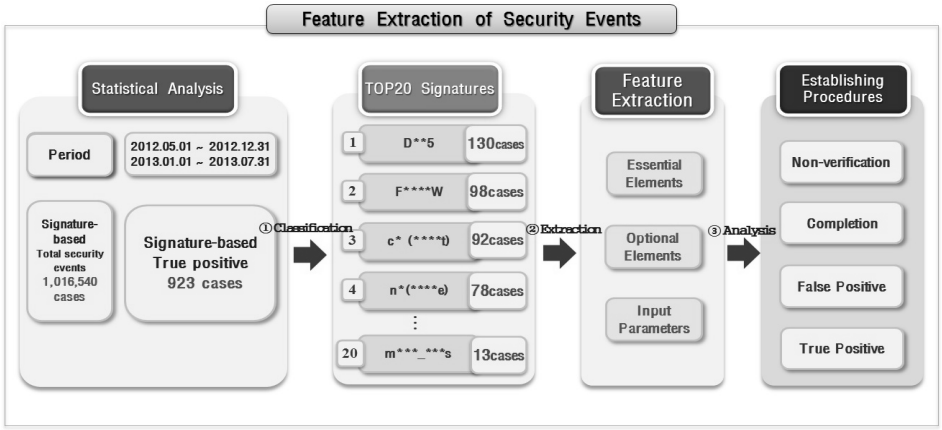


Fig.9. Feature Extraction Process of Security Events

Table 2. Features of Top20 Security Events

	Events	Feature
1	D**5	Transfer of system information by infection
2	F****w	Information transfer to compromised system
3	c*(****t)	Signal transfer to C&C server
4	n*(****e)	DDoS attacks by infection
5	i***-******t	Signal transfer or receiving response message to compromised system by infection
6	D******t	
7	n*****2010	
8	h****i	Information transfer to compromised system
9	R****g	URL connection to compromised system
10	D***.***t	Signal transfer to C&C server
11	e**.**l	Information transfer to compromised system
12	g****-******e	Signal transfer to C&C server
13	g*****.*5	Information transfer to compromised system
14	s*********-**** *1~2	Signal transfer to compromised system by infection
15		
16	c*******.2	
17	n*****-****i	DDoS attacks by infection
18	c**-*******e	Signal transfer to C&C server
19	s*****-*******n	Information transfer to compromised system
20	m***_***s	Signal transfer to C&C server

또한, 우리는 약 5~8개월 간 축적한 데이터를 확보하여 각 보안이벤트의 특징을 추출하였다. 보안이벤트의 특징추출 절차는 Fig.9에서 알 수 있듯이 우선, 앞서 추출한 20개의 보안이벤트를 바탕으로 수집된 보안이벤트에 대한 통계분석을 실시하였다. 그 결과, 문자열 기반인 보안이벤트 1,016,540건이 발생한 것으로 확인되었다. 이 중 923건의 정탐 보안이벤트(실제 사고처리건수)에 대한 원천 패킷 정보를 분석하고 정·오탐 판별을 위해 각 보안이벤트의 필수요소, 보조요소 및 입력값을 정의하여 관련 데이터를 추출하였다. 필수요소는 보안이벤트의 정·오탐을 결정하는 핵심요소이며 보조요소는 오탐을 줄이는 부가적인 정보이다. 입력값은 필수 및 보조요소의 실제 파라미터를 의미한다. 이들을 토대로 보안이벤트의 특징추출을 수행하고 추출된 2가지 요소 및 입력값의 정확도를 산출하기 위해 정·오탐 판별 및 사전 검증 등을 실시하여 자동검증 절차를 수립한다.

4.2 보안이벤트 특징추출 방법 및 절차

자동검증을 수행하기 위한 보안이벤트의 특징추출 방법은 Table.3와 같이 통계분석 및 정·오탐 판별 기준 등 7가지 분석 순으로 이루어진다. 우리는 해당 분석의 이해를 돕기 위해 사이버 해킹 공격 중 과학기술 분야에서 가장 빈번하게 대응지원을 수행 하였던 D**5* 이벤트를 예시로 들었으며 분석에 보다 밀접한 부분들은 관련 이벤트를 중심으로 서술하였다.

* D**5: 정보유출형 웜·바이러스 및 악성 프로그램에 감염된 시스템이 악성 도메인에 접속하여 추가 악성코드를 다운로드 하거나 MAC주소 및 OS 버전 등의 시스템 정보를 전송하는 행위를 탐지하는 이벤트

Table 3. Feature Extraction Methods of Security Events

	Item	Contents
1	Statistical Analysis	Basis analysis for security events of selected Top 20
2	True and false Analysis	Feature analysis for essential and optional elements
3	True Positive	Frequency analysis for essential and optional elements
4	Exception Process	Feature analysis for non-response events by the policy
5	Non-analysis	Feature analysis for untreated true positive events
6	False Positive	Feature analysis for false positive events
7	Input value Extraction	Parameter analysis for essential and optional elements

4.2.1 통계 분석

통계 분석은 정탐 보안이벤트에 대한 특징을 추출하기 위해 가장 먼저 수행되는 분석이다. 과학기술사이버안전센터(S&T-SEC)에서 수집된 보안이벤트를 기반으로 기본적인 통계자료를 도출하고 이를 통해 심층분석을 수행하는 기틀을 제공한다. Table.4는 통계분석을 위한 세부 항목을 나타낸다.

Table 4. Lists of Statistical Analysis

Item	Contents
Object	Analysis target
Period	Data gathering period
Number of security events	Total detection events
Number of redundancy	Security events that source IP is more than one
Number of unique	Security events deleted redundancy of source(destination) IP
Number of response	Responding security events
Number of re-response	Re-responding security events
Number of exception process	Non-response events by the policy
Number of false positive	Security events determined as false positive

실제 D**5 보안이벤트의 통계 분석 결과는 Table.5와 같으며 5개월간 발생한 이벤트를 대상으로 하였다. 다른 보안 이벤트의 경우 통계분석이 가능한 최소한의 데이터 수집이 필요하기 때문에 수집 기간이 상이할 수 있다. D**5 통계분석에서 특이한 부분은 재사고(탐지) 건수이다. 재사고 건수 비율은 140%로 상당히 높은 수치를 기록하였다. 이는 임의의 시스템이 최초 D**5에 감염이 된다면 또다시 재감염된다는 사실을 알 수 있다. 또한 c*(****t) 보안이벤트의 경우, 시스템 감염 후 지령서버로 감염 신호를 송·수신하는 행위로 인해 장시간 동안 지속 발생하기에 발생빈도수가 유사 이벤트보다 큰 편이라는 사실을 통계분석을 통해 도출되었다.

Table 5. Results of Statistical Analysis

Item	Contents
Object	Gathering security events through TMS in S&T-SEC
Period	2012. 5. 1. ~ 2012. 9. 30.
Number of security events	507 cases
Number of redundancy	337 cases
Number of unique	170 cases (Source IP redundancy removal)
Number of response	318 cases(May: 56(36.1%), June: 73 (45.9%), July: 45(31.7%), August: 53 (39.6%), September: 91(25.8%))
Number of re-response	186 cases (140%)
Number of exception process	38 cases
Number of false positive	0 cases

4.2.2 정·오탐 판별

정·오탐 판별은 자동검증을 위한 필수요소 및 보조요소를 추출하여 정·오탐 여부를 결정하는 과정이다. Table.6은 정·오탐 판별을 위해 필수 및 보조요소를 정의한 것이며 이전 단계의 통계분석에서 도출된 데이터를 기반으로 정·오탐 판별의 기준이 되는 요소를 추출한다.

Table 6. True positive and False positive Analysis

Item	Contents
Essential Elements	Elements to determine true positive and false positive
Optional Elements	Elements to reduce false positive

D**5의 경우 필수 및 보조요소 추출은 Table.7과 같으며 보안을 위해 일부분만을 예시로 들었다.

Table 7. Essential and Optional Elements of D**5

Item	Element	Contents
Essential elements	Source IP	Monitoring institutes
	Destination IP	Compromised system
	MAC Address	System address
	OS	Operating System
Optional elements	Ver	HTTP version
	User-Agent	Connection program
	Host	Destination address

4.2.3 정탐분석

본 단계에서는 정·오탐을 결정하는 필수 및 보조요소의 발생빈도를 측정하여 추출된 요소들의 적합성을 검증하는 분석이다. Table.8은 필수(보조)요소의 정탐분석에 대한 정의를 나타내며 해당분석을 통해 만약 추출한 필수(보조)요소의 정탐비율이 낮을 경우 이전 단계를 반복 수행하여 필수(보조)요소를 다시 추출하게 된다.

Table 8. Analysis of True positive events

Item	Contents
Unit	Unit item of essential and optional element
Ratio	Ratio of unit item

Table.9은 3가지 보안이벤트에 대한 실제 정탐분석 결과를 보여준다. D**5 보안이벤트의 경우 필수 및 보조요소가 100%일치하는 것을 확인할 수 있음에 반해 n*(****e) 보안 이벤트의 Pragma 요소비율은 23%로 상대적으로 낮은 수치가 도출되었다. 이 경우 정·오탐 판별을 재 수행하여 필수(보조)요소를 추출하거나 분석수집 기간을 확대하여 정탐비율을 재계산한다.

Table 9. Results of Three True Positive Events

Event	D**5	m***_***s	n*(****e)
Unit item	MAC (100%)	Memory size (100%)	Agent (100%)
	OS (100%)	Memory clock (100%)	Ver (100%)
	Ver (100%)	Packet size (100%)	Pragma (23%)
	Agent (100%)	Specific char (51%)	Host (100%)

4.2.4 예외처리 분석

탐지이벤트가 정탐으로 판별되었으나 정책에 의해 사고처리를 진행하지 않은 이벤트로 Table.10은 예외처리 항목을 보여준다.

Table 10. Lists of Exception Processing

Item	Contents
Institute requirement	- Exception bandwidth by institute requirement
Test section	- Malware collection and analysis bandwidth
Non-monitoring institutes section	- Bandwidth out of security monitoring

위의 예외항목을 토대로 Table.11는 총 13건의 D**5 예외처리를 나타난 결과이다.

Table 11. Results of D**5 Exception Processing

Classification	Institute requirement	Test	Non-monitoring
Exception	10 cases	3 cases	0 cases

4.2.5 미처리 분석

미처리 분석은 예외처리 분석 결과 실제 해킹공격으로 사고처리를 진행해야 함에도 불구하고 대응하지 못한 이벤트를 의미한다. 우리는 미처리 분석을 위해 Table.12와 같이 미처리 분석에 필요한 항목을 도출하여 미처리에 대한 사유를 판별한다.

Table 12. Lists of Untreated Events

Item	Contents
Packet	- Detected packet value
Attacker (IP)	- Attacker's IP address
Response history	- Response history of security event
Result	- Analysis result of each item

D**5의 미처리 분석은 Table.13에서 확인할 수 있으며 전체의 패킷내용 중 일부분만을 기술하였다. 미처리 건수는 11건으로 실제 보안관제 요원이 처리하지 못한 이벤트이다. 해당수치는 하루 수천 건의 보안이벤트가 탐지되는 상황에서 미비한 수치로 보일 수 있으나 보안위협 수준에 따라 강도가 달라질 수 있기 때문에 보안이벤트의 자동검증 시스템 구축의 시급성을 나타내주는 예시라 하겠다.

Table 13. Analysis of Untreated D**5 Events

	Packet (Part)	Attacker IP	Response history	Result
1	GET./xx/get.mac=B****..&os=winxp%20Profession&ver=HTTP/1.1..User-Agent:Google.page…	203.x.x.x	No	Examples that operator don't analysis these events
2	GET.get.mac=4*********…&os=Windows%207&ver=NO..HTTP/1.1..Host:69.46.x.x··	210.x.x.x	No	
8 other cases				

4.2.6 오탐 분석

오탐분석은 정탐으로 탐지되었으나 관제요원의 분석결과 오탐으로 확인된 이벤트에 대상으로 분석을 실시한다. 오탐분석을 위해 도출된 항목은 Table.14와 같으며 위에서 언급된 미처리 분석과 유사하다. 한 가지 다른 부분은 오탐판정 항목이다. 보안관제 요원이 해당 이벤트에 대해 오탐 결정을 내린 사유와 오탐 이력을 바탕으로 최종 분석이 이루어진다.

Table 14. Lists of False Positive events

Item	Contents
Packet	- Detected packet value
Attacker (IP)	- Attacker's IP address
Result	- False positive result

Table.15은 상위 20종의 보안이벤트 중 d******t, c*(****t) 및 s********s-n*****1 보안이벤트에서 오탐이 발생하는 예시이다. 우선 d******t 이벤트는 탐지패턴 조건의 ver요소 등 일정부분만을 부합한 오탐이었으며 c*(****t) 이벤트는 웹페이지의 문자열 탐지로 인한 오탐인 것으로 확인되었다. 또한, s********s-n*****1 보안 이벤트의 경우 윈도우 또는 소프트웨어 업데이트 시에 발생한 탐지로 판별되었다.

Table 15. Results of 3 False Positive events

Security Events	Packet (Part)	Attacker IP	Result
d******t	……N:……url mon.dll..URLDownloadToFileA..&ver=…clcount/count.asp…	210.x.x.x	False positive
c*(****t)	..E….S@.5.+D..s….8…..a…..C…6……..H…..8G****w0lf".class="author.id-t2_5pnn7".〉	210.x.x.x	
s********_*****1	….Windows.Installer……Hwp2004……Hwp2004……Haansoft……Install,MSI··	203.x.x.x	

4.2.7 입력 값 추출

본 단계에서는 탐지된 정탐이벤트에 대한 필수요소 및 보조요소의 실제 파라미터를 추출하고 입력 값의 발생빈도 등을 파악하여 필수요소 및 보조요소의 정확도를 검증한다. Table.16은 입력 값 추출을 위한 항목을 정의한다.

Table 16. Lists of Input Value

Item	Contents
Unit	- Unit item for Essential and optional elements
Content	- Description for each unit item
Input value	- Parameter for each unit item
Ratio	- Frequency for each unit item

실제 D**5의 입력값 추출 결과는 Table.17에서 보여준다.

Table 17. Extractions of D**5 Input Value

	Unit	Contents	Input value	Ratio
Essential elements	Source IP	Institute	Institute IP	100%
	Destination IP	Compromised system	IP	
	MAC	System address	Hex	100%
	OS	Operating System	Windows%xp	98%
			win7	1%
			unknown	1%
Optional elements	ver	HTTP version	.HTTP/1.1	98%
			etc	2%
	User-Agent	Connection Program	Google.page	97%
			Mozilla/3.0	1%
			etc	2%
	Host	Destination IP	IP	48%
			Host	52%

V. 보안이벤트 자동검증 시스템 구축

5.1 보안이벤트 자동검증 절차

앞선 보안이벤트의 특징추출의 결과를 구조적으로 정형화하기 위해 자동검증 절차를 수립한다. Fig.10은 D**5 이벤트의 플로 차트를 나타내며 정·오탐 검증은 각 보안이벤트의 필수요소 및 보조요소를 통해 결정된다. 해당 보안이벤트에 대한 필수요소 검증을 수행한 후 2차적으로 보조요소 검증을 진행한다. 만약 2차 보조요소가 부합되지 않은 이벤트에 대해 관제요원의 확인하는 과정을 거친다.

5.2 사전검증

본 단계에서는 지금까지 수행한 분석 결과의 신뢰성을 입증하기 위해 일정기간 동안 사전검증에 필요한 보안이벤트의 필수요소, 보조요소 및 입력 값을 추출하여 정확도를 검증한다. 자동검증시스템 구축 전에 사전검증을 수행함으로써 정확도 예측이 가능할 뿐만 아니라 추출 요소 이외에 다른 부가적 요소 확인도 가능하다. D**5의 경우, 추출된 해당이벤트의 필수요소, 보조요소 및 입력값 모두 일치하였으며 별도로 추가해야 할 요소를 발견하지 못했다.

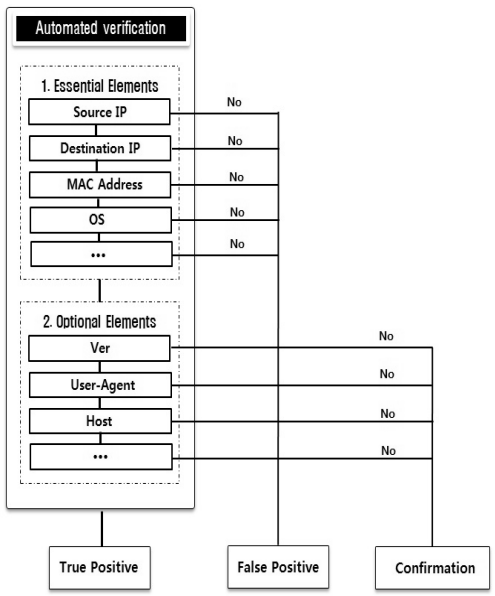


Fig.10. Automated Verification Procedure of D**5 True and False Detection

5.3 자동검증 시스템 구성

본 연구에서는 과학기술연구망 및 보안관제 대상 기관으로부터 유입된 침해위협 트래픽을 기반으로 기 구축된 침해위협관리시스템(TMS) 및 종합정보분석 시스템(SMART)과 연동하여 실시간으로 탐지된 보안 이벤트에 대한 자동검증시스템을 시범구축 하였다. 보안이벤트 자동검증 시스템의 전체적인 구성은 Fig.11와 같다.

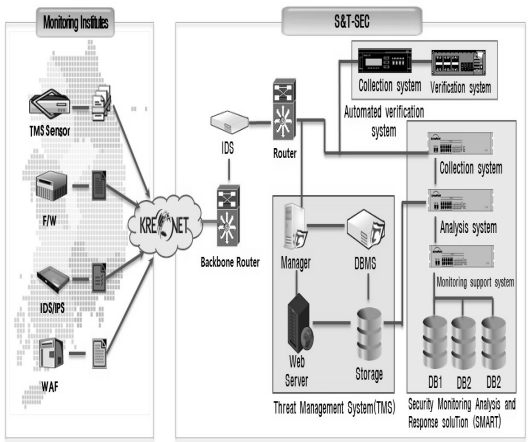


Fig.11. Configuration of Automated Verification System

지역망 센터 및 보안관제 대상기관에 설치된 보안 장비(TMS센서, 방화벽, IPS 등)로부터 각 특성에 해당하는 데이터를 수집한다. 이들 데이터에서 수집된 침해위협 트래픽은 침해위협관리시스템(TMS)으로 전송하여 정·오탐 여부를 판별하고 침해로그 정보들은 종합정보분석시스템으로 보내져서 상관분석을 통해 대량의 보안이벤트를 축약·필터링하여 무의미한 이벤트를 제거하는 역할을 수행한다. 자동검증시스템은 보안 이벤트 양을 감소시키는 것에 초점을 맞추기 보다는 실제 사람에 의해 해킹피해 여부를 자동으로 분석·판단하는 차세대 보안관제 및 침해대응 기술이다.

5.4 보안이벤트 자동검증 시스템 설계

보안이벤트의 정·오탐 판별 여부를 자동으로 판단하는 자동검증 시스템 설계는 Fig.12와 같다. 자동검증 시스템 이벤트의 처리 프로시저는 4가지(수집, 분류, 분석 및 사고검증)의 에이전트로 구현하였으며 절차는 다음과 같다.

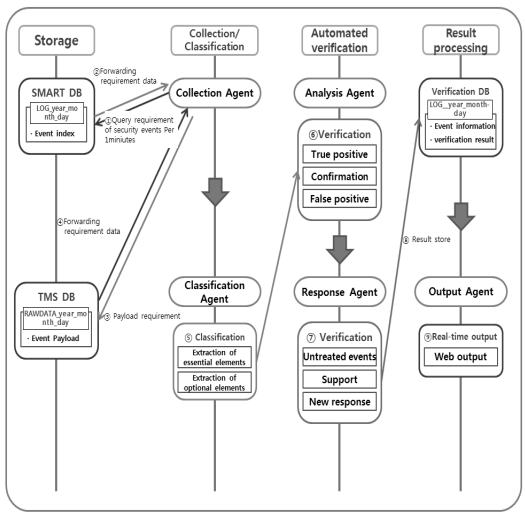


Fig.12. Procedures of Automated Verification System

① 수집 에이전트는 1분마다 새로 발생하는 탐지 이벤트를 가져오기 위해 종합정보분석시스템(SMART) DB에서 인덱스 번호를 요청한다.
② 종합정보분석시스템은 수집 에이전트에게 해당 번호를 전송한다.
③ 수집 에이전트는 전송받은 인덱스 번호를 바탕으로 탐지 이벤트의 실질적인 분석을 위한 원천 데이터를 가져오기 위해 침해위협탐지시스템(TMS) DB로부터 관련정보를 요청한다.
④ 침해위협관리시스템은 수집 에이전트에게 해당 정보를 전달한다.
⑤ 분류 에이전트는 수집 에이전트에게 넘겨받은 관련수집 정보를 토대로 RAWDATA에서 1차 필수요소 및 2차 보조요소 값을 추출한다.
⑥ 분석 에이전트는 분류 에이전트에서 추출한 항목을 토대로 탐지 이벤트의 정·오탐 유무를 확인한 후 해당 값을 검증 에이전트로 전송한다.
⑦ 사고 검증 에이전트는 해당 이벤트의 IP를 확인하여 예외처리 여부를 결정한다.
⑧ 도출된 검증 결과를 바탕으로 DB를 생성한다.
⑨ 해당 DB를 참조하는 자동검증 웹 뷰어를 구축한다.

5.5 보안이벤트 자동검증 시스템 주요 함수 및 구현

자동검증 시스템은 각 이벤트의 검증 클래스를 실행시키는 「시작 클래스」, 각 이벤트의 정·오탐 여부를 판별하는 「분석 클래스」와 정탐 판별 후, 예외처리 여부를 판별해주는 「예외처리 클래스」로 구성된다. Table.18은 프로그램 시작 클래스의 주요 함수를 보여준다. 시작 클래스는 총 20개의 이벤트에 대해 각 클래스를 생성한 후 쓰레드(Thread)에 넣어준다. 단일 쓰레드로 작성할 경우 순차적으로 20개의 이벤트에 대해서 검증하기는 비효율적이다. 따라서, 시스템 효율을 향상시키기 위해 20개의 쓰레드를 생성하여 동시에 모든 이벤트에 대해 검증을 실시한다.

Table 18. Start Class of Automated Verification System of D**5

Start Class Function

/* Analysis class execution of each security events */
void main( ) {
// Verification class creation of D**5 event
event_D**5 D**5 = event_D**5( );
 	
//Thread creation of D**5 event
Thread D**_thd = new Thread(D**5);
 	
//Thread execution
D**5_thd.start( );

Table.19는 검증 이벤트 중 D**5 이벤트의 정·오탐 여부를 판별하는 분석 클래스의 주요 함수를 보여준다. 검증 클래스에서 정·오탐 판별 유무를 가려낸 후 뷰어 시스템에서 활용하는 검증완료 이벤트 DB에 저장하는 과정까지 거친다. 각 이벤트는 HEX값과 ASCII 코드로 변형된 값을 사용하여 정·오탐을 판별한다.

Table 19. D**5 Verification Class of Automated Verification System

Verification Class Function

/* Analysis class execution of each security events */
void main( )
{
…
//DB connection function to call SMART DB
Statement Smart_stmt = Smart_conn.createStatement();
 	
//DB connection function to call TMS DB
Statement tms_stmt = tms_conn.createStatement();
 	
//Query to call SMART DB
ResultSet smart_log_rs = Smart_stmt.executeQuery();
 	
//RAWDATA collection and verification of security events
while (Smart_log_rs.next()) {
 	
//Function to call events number of SMART DB
smart_log_rs.getInt("xxx");
 	
//Step to call RAWDATA based on security event number
ResultSet tms_rawdata_rs = tms_stmt.execute Query();
tms_rawdata_rs.next();
tms_rawdata_rs.getString("yyy");
…
//True and false distinction after changing RAWDATA into ACSII
ASCII_check()
…
 	
//Event result store in completion DB
mysql_strnt.executeUpdate();
}
ASCII_check() {
 	
//Item extraction of automated verification to RAWDATA
get_value();
…
 	
//Item distinction in RAWDATA
ASCII_equals();
}
HEX_check() {
 	
//Feature extraction and distinction of IP, MAC, Protocol and etc
HEX_equals();
…
}

Table.20은 검증 클래스의 주요 함수를 보여준다. 검증 클래스(IP_verification.java)는 모든 정탐 이벤트에 대해서 검증 IP의 예외처리 여부를 판단한 후 해당 이벤트 클래스에 결과를 전송한다.

Table 20. Exception Class of Automated Verification System

Exception Class Function

/* Exception processing verification */
void main( )
{
//DB connection function for to call exception IP list
Statement Smart_stmt = Smart_conn.Create Statement();
//Function to call test bandwidth
Verification_rs = Smart_stmt.executeQuery();
…
 	
//Function to call response history IP
Tosimtm_rs = tosimtm_stmt.executeQuery();
…
//Verification function for response history IP and test bandwidth
IP_check();
…
//Flag value return after checking exception IP
retrun result;

Fig.13은 기존의 보안이벤트 탐지 뷰 화면이며 Fig.14는 제안한 자동검증 결과 값을 반영한 뷰 화면이다.

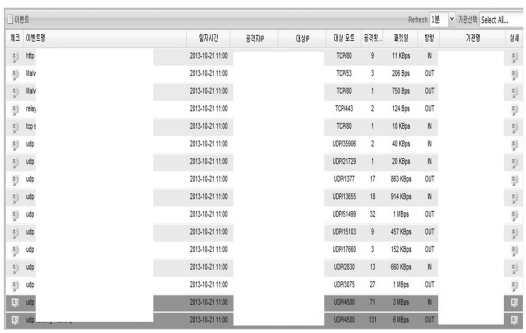


Fig.13. A Screenshot of Viewer System - Before

제안 뷰는 Top20 보안이벤트에 대해 자동검증을 수행하고 자동검증을 마친 이벤트에 대해 관제 모니터링 뷰에 플래그(Flag)를 적용하여 하위 보안이벤트와 구별이 가능하도록 구현하였다. 이로 인해 보안관제 수행 화면의 가독성을 증가하였다.

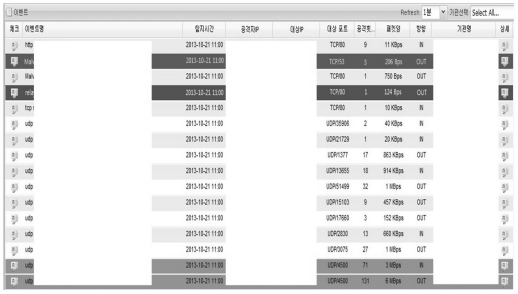


Fig.14. A Screenshot of Viewer System - After

VI. 보안이벤트 자동검증 시스템 결과분석

이 장에서는 자동검증 시스템의 결과분석을 통해 검증 정확도 및 보안관제 업무의 신속성 등의 우수성을 입증하고자 한다.

6.1 보안이벤트 자동검증 시스템 정확성 향상

우선, 과학기술분야에서 발생하는 사이버 침해공격 중 해킹시도 발생빈도가 높은 상위 20종의 보안이벤트에 대한 자동검증 기술 개발을 완료하였으며, 이를 기존 보안관제 체계에 시범적용하여 약 98.8%의 자동검증 정확도를 보였다. Fig.15는 Top20 보안이벤트의 정확도를 나타낸다. 17개의 이벤트에 대해 100%의 정확도가 도출되었으며 나머지 3개의 이벤트의 경우에도 높은 정확도를 얻었다.

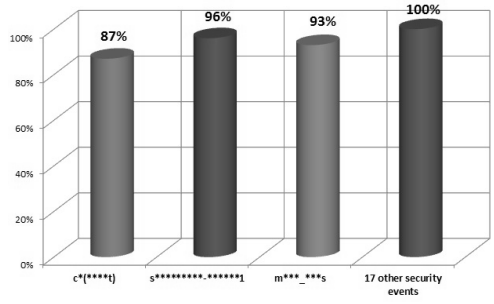


Fig.15. Accuracy of Automated Verification System

또한 Fig.16과 같이 기존 보안관제 체계에서 보안관제 요원이 발견하지 못한 140건의 실제 해킹 공격에 대해서도 본 연구의 자동검증 기술을 적용함으로써 해당 사이버 해킹공격을 문제없이 발견 및 대응하여

정확성을 향상시켰다.

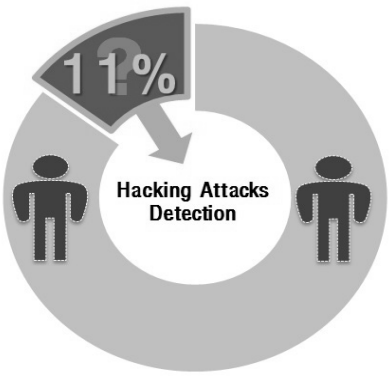


Fig.16. Responding Non-Detection by Automated Verification System

6.2 보안이벤트 자동검증 시스템 신속성 향상

Fig.17은 보안이벤트 자동검증의 신속성을 나타낸다. '12년도 과학기술사이버안전센터의 사고처리 건수는 총 2097건이며 Top20 보안이벤트에 대한 분석기간이 평균 7개월(611건)임을 감안할 때 해당 개월 수로 계산한 결과 전체의 약 50%에 대해 보안관제 요원의 추가적인 분석을 거치지 않고 실제 해킹공격 발생여부를 자동으로 판단 가능하게 되었으며 결과적으로 보안관제 요원의 업무량을 50% 수준으로 감소시켰다.

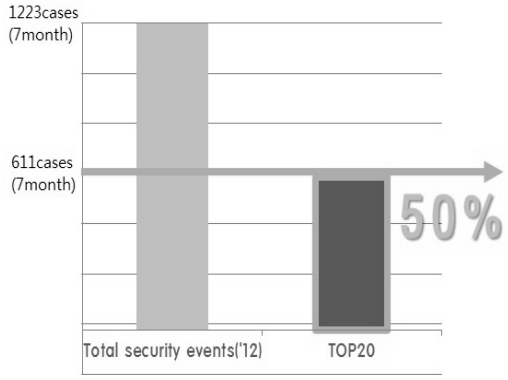


Fig.17. Reduced Workload of Automated Verification System

VII. 결 론

대용량 보안이벤트에 대한 탐지 및 분석업무의 효율성을 향상시키기 위한 연구가 국내·외에서 진행되어 왔으나 이들 연구의 대부분은 보안이벤트에 대한 기본정보(IP, 포트, 프로토콜, 이벤트 명 등)만을 이용하여 사이버위협 동향 파악 및 분석 대상 보안이벤트 수를 감소시키기 위한 간접적 접근(통계분석, 가시화 등)에 초점을 맞추고 있었다. 이로 인해 보안이벤트에 대한 실제 해킹공격 발생여부를 판단하기 어려워 보안관제 업무 수행 시 추가적인 분석이 필요하였다.

반면, 본 연구는 실제 해킹시도와 관련된 실제 트래픽 정보를 이용하여 보안이벤트를 자동으로 분석하고 이를 통해 실제 해킹 공격 발생여부를 실시간으로 판단하기 위한 자동검증 기술을 제안하였다. 실제 해킹 시도와 관련된 보안이벤트를 자동으로 분석·검증함으로써 보안관제 업무의 효율성 향상에 직접적인 기여가 가능할 뿐만 아니라 원천데이터 활용을 통해 해킹공격에 대한 정확한 탐지 및 분석 업무 수행이 가능하였다. 본 연구를 통해 개발된 보안이벤트 자동검증 시스템은 현재 과학기술사이버안전센터(S&T-SEC)를 통해 시범 적용 중이며 해당 기술의 안정화·고도화를 위해 실시간 보안관제 및 침해대응 서비스에 적극 활용할 예정이다.

References

[1] Yu, D. and Frincke, D., "A Novel Framework for Alert Correlation and Understading," Proc. on ACNS 2004, LNCS 3089, pp. 452-466, Jun. 2004.

[2] Debar, H. and Wespi, A., "Aggregation and Correlation of Intrusion-Detection Alerts," Proc. on the 4th International Symposium on Recent Advances in Intrusion Detection (RAID), Springer Verlang, pp. 85-103 Oct. 2001.

[3] Giacinto, G., Perdisci, R. and Roli, F., "Alarm Clustering for Intrusion Detection Systems in Computer Networks," Proc. on MLDM 2005, LNAI 3587, pp 184-193, July. 2005.

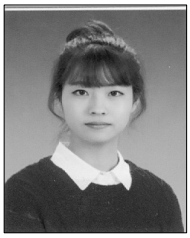
[4] Ning, P., Cui, Y. and Reeves, D.S., "Analyzing Intensive Intrusion Alerts via

Correlation," Proc. on the 5th International Symposium on Recent Advances in Intrusion Detection (RAID), Springer Verlang, pp. 74-94, Oct. 2002.
〔5〕 Y. Livnat, J. Agutter, S. Moon, and S. Foresti, "Visual Correlation for Situational Awareness," Proc. of IEEE 2000 Symp. on Information Visualization (InfoVis), pp. 95-102, Oct. 2005.
〔6〕 K. Lakkaraju, W. Yurcik, and A. Lee, "NVisionIP: Netflow Visualization of System State for Security Situational Awareness," Proc. of VizSEC 2004, ACM Press, New York, NY, USA, pp.65-72, Oct. 2004.
〔7〕 Science&Technology Security Center, http://www.sntsec.or.kr/
〔8〕 Ning, P., Cui, Y. and Reeves, D.S., "Constructing Attack Scenarios through Correlation of Intrusion Alerts," Proc. on the 9th ACM conference on Computer and Communications Security, pp. 245-254. Nov. 2002.
〔9〕 Ning, P., Xu, D., Healey, C.G. and Amant, R.S., "Building Attack Scenarios through Integration of Complementary Alert Correlation Methods," Proc. on the 11th Annual Network and Distributed System Security (NDSS '04), pp. 97-111, Feb. 2004.
〔10〕 Ning, P., Cui, Y., Reeves, D.S. and Xu, D., "Techniques and Tools for Analyzing Intrusion Alerts," ACM Transactions on Information and System Security, pp. 274-318, May. 2004.
〔11〕 Al-Mamory, S.O. and Zhang, H., "IDS Alerts Correlation Using Grammar-based Approach," Journal in Computer Virology 5(4), pp. 271-282, Aug. 2008.
〔12〕 Song, J., Takakura, H. and Kwon, Y., "A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts," Proc. on SAINT 2008, IEEE CS Press, pp. 51-56, July. 2008.
〔13〕 Ho-sub Lee, Eung-ki Park, Jung-taek Seo., "A New Method to Detect Anomalous State of Network using Information of Clusters," Journal of The Korea Institute of Information Security & Cryptology vol. 22, no. 3, pp. 545-552, Jun. 2012.
〔14〕 Pedro Casa, Johan Mazel, Philippe Owezarski,. "Unsupervised Network Intrusion Detection Systems: Detecting the Unknown without Knowledge," Computer Communications Journal of Elsevier, pp 772-783, April. 2012.
〔15〕 HoonJae Lee, "A study on generalization of Fault-Injection Analysis tools," 2013-046, Dongseo University Industry-Academic Cooperation Foundation, 2013.

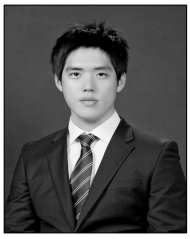
〈저 자 소 개〉

김 규 일(Kyu-il Kim) 정회원
2005년 2월: 성균관대학교 컴퓨터공학과 석사
2010년 2월: 성균관대학교 컴퓨터공학과 박사
2010년 6월~현재: 한국과학기술정보연구원 과학기술정보보호실 선임연구원
〈관심분야〉 보안관제, 침해사고대응, 악성코드 분석

박 학 수 (Hark-soo Park) 정회원
1989년 2월: 한남대학교 전자계산학과 졸업
1991년 2월: 한남대학교 컴퓨터공학과 석사
2003년 2월: 한남대학교 컴퓨터공학 박사
1991년 3월~현재: 한국과학기술정보연구원 책임연구원
〈관심분야〉 정보보호, 보안관제, 침해사고대응



최 지 연 (Ji-yeon Choi) 학생회원
2013년 2월: 한남대학교 경영정보학과 졸업
2013년 3월~현재: 과학기술연합대학원대학교 그리드 및 슈퍼컴퓨팅 석사과정
〈관심분야〉 정보보호, 악성코드 분석, 네트워크 보안



고 상 준 (Sang-jun Ko) 학생회원
2013년 2월: 한국항공대학교 정보통신공학 졸업
2013년 3월~현재: 과학기술연합대학원대학교 그리드 및 슈퍼컴퓨팅 석사과정
〈관심분야〉 정보보호, 네트워크 보안, 악성코드 분석

송 중 석 (Jung-suk Song) 정회원
2003년 2월: 한국항공대학교 통신정보공학 졸업
2005년 2월: 한국항공대학교 정보공학 석사
2009년 3월: 교토대학교(일본) 지능정보학 박사
2009년 4월~2010년 9월: 일본정보통신연구원 정보통신 보안 연구소 전문연구원
20010년 10월~2011년 9월: 일본정보통신연구원 네트워크 보안 연구소 선임연구원
2011년 10월~현재: 한국과학기술정보연구원 과학기술정보보호실 선임연구원
2012년 9월~현재: 과학기술연합대학원대학교 그리드 및 슈퍼컴퓨팅 조교수
〈관심분야〉 보안관제, 침해사고대응, 악성코드 분석, 네트워크 보안