U-city 사이버 테러 방지를 위한 예·경보 알고리즘에 관한 연구
forecast and Warning Algorithm for U-city cyber terror protection

김 형 중*, 정 규 일**, 이 준 엽***
Hyoung-Jung kim, Kyou-il chung, and Jun-Yeop Lee

Abstract

This thesis offers forecast & warning algorithm about the accessing networks though statistical sampling methods to prevent computer terrors. These networks are occurred among U-city network groups.

The main characteristic of current computer attacks is avoiding well-known detection patterns by successive changes in spreading speeds and attacking codes. The improvement of attacking skills leads to a problem causing the defense-time delay and creates vicious cycle that tries to fix networks after damage. Proposed algorithm notices and warns the potential attacking areas through detecting previous attacking signs, analysing attacking results and tracing attacking sources at the beginning of the attack.

Keywords : C&C (command & contorl), 악성코드, 좀비 PC, DDos, 네트워크 트래픽 통계 분석

I. 서 론

침입 탐지 시스템, 침입 차단 시스템, 웹 방화벽, 백신 프로그램은 수집된 공격 패턴 비교를 통한 공격 검출 및 차단 기술을 핵심으로 하고 있다.

이와 같은 기술은 알려진 공격에 대한 확산을 방지 하고, 이미 침해된 시스템 복구에 필수 적이 보안 기술 이다.

그러나 이러한 보안 기술은 이미 파급된 공격에 대한 공격 기법을 분석하여 방어를 수행 하는 것을 근간으로 하고 있어 현재와 같이 공격자가 기존의 탐지 가능한 코드 패턴의 탐지 범위를 회피할 수 있도록 다양하게 변형된 공격 코드를 빠른 주기로 제작 배포하여 다수의 개인 PC를 좀비 PC화하여 공격을 수행하는 상황에서의 차단 및 방지 대책에 대한 실효성이 감소되고 있다.

DDos 탐지 및 네트워크 트래픽 분석 기술은 패턴 방식의 검출 기술의 한계성을 탈피하고 이상 트랙픽 감지 및 서비스 이용 패턴 분석을 통한 공격 탐지 및 방어를 수행함으로서 패턴 탐지 기반의 보안 기술을 보강하고 있으며 개별 네트워크 및 서비스 단위에서의 실효성을 발휘하고 있다.

DDos 탐지 기술은 서비스 제공자가 자신의 서비스 시스템 보호를 위하여 구축 운영하는 형태로 전개 되고 있으며, 트래픽 분석 기술은 이상 트패픽 발생 감지를 이용한 내부 네트워크 보호 방향으로 구현되고 있다.

이러한 기술의 발전 방향은 개별 서비스 또는 네트워크 단위의 보안 강화를 확보 할 수 있으나 복수 지역에 걸쳐 발생하는 공격 및 감염에 대한 분석 및 통계 추출의 문제점을 갖게 된다.

따라서 본 논문에서는 U-City로 대표되는 복수 네트워크 집합체간에 발생하는 네트워크 이용에 대한 사이버 테러 방지에 적용하기 위한 예·경보 알고리즘을 다음과 같이 구분하여 제안한다.

- ○ 예·경보 알고리즘
- ○ 예·경보 오차범위 보정 알고리즘
- ○ 근원지 및 감염 예상 PC 추적 알고리즘
- ○ 피해 예상 규모 추정 및 파급 경로 분석

접수일자 : 2009년 7월 31일
최종완료 : 2009년 7월 27일
*고려대학교 정보경영전문대학원
**숭실대학교 전기제어시스템공학부
교신저자, E-mail : edit@itfe.or.kr
***(주)시큐에버

II. 예·경보 알고리즘

본 논문에서의 공격 예측 알고리즘의 적용은 Internet Protocol의 전송계층 프로토콜인 TCP와 Non TCP로 구분하고, 이용자의 네트워크 자원 이용을 위한 행위로 DNS 접속과 IP 직접 입력으로 구분한다.

공격 예측 알고리즘은 그림 1로 표현되는 방식에 의하여 구분된 화이트 리스트를 생성하게 되고 생성된 화이트 리스트의 검출 빈도에 따른 블랙 리스트를 생성하여 예·경보 대상으로 적용된다.

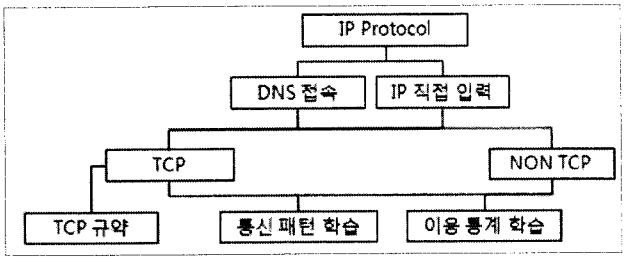


그림 1. 예·경보 알고리즘 적용
Fig. 1. Forecasting And Warning Algorithm Apply

1. DNS 접속 분석 예·경보 알고리즘

DNS는 URL을 이용한 네트워크 자원의 접근을 위하여 반드시 접속하여야 하는 서비스로서 이용자가 질의한 URL의 IP 주소를 응답하여 주는 서비스를 담당한다.

URL을 이용한 예·정보 알고리즘 다음과 같은 URL 이용 특징에 대한 화이트리스트의 작성을 수행 한다.

(i) 통계 집단에서 사용하는 DNS는 일정한 범위이내의 URL 목록을 이용한다.
(ii) 통계 집단에서 사용하는 특정 URL의 이용 통계는 일정 범위 안에 존재한다.
(iii) 통계 집단을 기준으로 일정 비율 이내의 사용자에 의한 급격한 이용 증가를 보이는 URL은 자동화된 공격을 의심 한다.
(iv) 특정 URL의 응답 IP는 일정한 범위에서 제공된다.
(v) 단기간 이용되다 소멸되는 URL은 비정상적인 서비스의 확률이 높다.
(vi) 기계적 주기성을 갖고 호출되는 URL는 비정상적인 서비스의 확률이 높다.

2. 목적지 IP 분석 예·경보 알고리즘

목적지 IP 접속 분석 예·경보 알고리즘은 네트워크 자원의 접근을 위하여 목적지 IP를 직접 입력하는 경우에 대한 분석 알고리즘 이다.

목적지 IP 접속 분석 알고리즘은 다음과 같은 이용 특징에 대한 화이트리스트 작성을 수행한다.

(i) 통계 집단에서 사용하는 IP는 일정한 범위이내의 URL 목록을 이용한다.
(ii) 통계 집단에서 사용하는 특정 IP의 이용 통계는 일정 범위 안에 존재한다.
(iii) 통계 집단을 기준으로 일정 비율 이내의 사용자에 의한 급격한 이용 증가를 보이는 IP은 자동화된 공격을 의심 한다.
(iv) 단기간 이용되다 소멸되는 IP은 비정상적인 서비스의 확률이 높다.
(v) 기계적 주기성을 갖고 호출되는 IP는 비정상적인 서비스의 확률이 높다.
(vi) 통계 집단의 특정 IP 그룹 내의 사용자 집단 IP내에서 사용자 집단 IP이외의 URL이 할당되지 않은 IP로의 직접 접근은 비정상적 서비스로의 접근 확률이 높다.

3. 출발지 IP 분석 예·경보 알고리즘

출발지 IP 분석 예·경보알고리즘은 네트워크에 위치한 사용자 IP를 기준으로하는 분석 알고리즘이다.

출발지 IP 분석 예·경보 알고리즘은 다음과 같은 이용 특징에 대한 화이트 리스트 작성을 수행한다.

(i) 통계 집단의 특정 IP 그룹 내의 사용자 집단 IP는 일정한 범위 이내의 전송 계층 프로토콜을 사용한다.
(ii) 특정 IP에서 발생하는 네트워크 트래픽은 일정 범위 이내에 존재 한다.
(iii) 특정 IP가 사용하는 DNS 질의 횟수는 일정 범위 이내에 존재한다.
(iv) 이용자에 의한 정상적 사용의 경우 시간적 주기성의 오차가 적은 반복 사용이 이루어지지 않는다.

4. TCP 규약에 의한 예·경보 알고리즘

TCP 규약에 의한 예·정보 알고리즘은 다음과 같은 이용 특징에 대한 화이트 리스트 작성을 수행한다.

(i) 모든 연결은 three-way handshake 방식을 이용하여 성립되며, SYN 요청 없이 발생하는 패킷은 위·변조된 패킷의 확률이 높다.
(ii) FIN 요청에 의하여 종료된 연결 이후에 발생하는 패킷은 위·변조된 패킷의 확률이 높다.
(iii) sequence 번호의 중복 발생 패킷은 위·변조 시도가 발생하고 있는 패킷의 확률이 높다.
(iv) 출발지와 목적지가 동일한 패킷은 위·변조된 패킷의 확률이 높다.
(v) 응답 없는 요청의 계속 또는 통계 비율 이상이 나타나는 연결은 공격에 사용되는 확률이 높다.
(vi) RST의 반복적 발생은 공격에 사용되고 있을 확률이 높다.
(vii) 외국 소유 IP는 일정한 통계 이내의 이용률을 보인다.

5. 통신 패턴 학습에 의한 예·경보 알고리즘

U-City 서비스에 사용되는 센서 통신 및 인터넷 상의 서비스 이용을 위한 요청 패턴은 응답 패턴 보다 산술적으로 적은 규모의 범위를 나타내게 된다.

이러한 요청 패턴을 분리하면 다음 그림과 같이 분석된다.

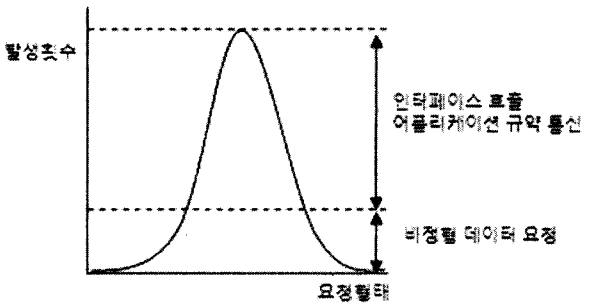


그림 2. 요청 패턴 분석
Fig. 2. analysis of request pattern

특정 서비스 이용을 위한 요청 데이터는 서비스 이용을 위한 규약 통신 또는 인터페이스 구성에 의한 이용 요청 데이터 통신이 복수의 사용자에게서 동일하게 반복되어 높은 발생 횟수를 나타내고, 서비스 제공자와 이용자 간의 특정 데이터 송수신은 개별 사용자의 행위에 따라 낮은 발생 회수를 나타내게 된다.

통신 패턴 학습은 전체 발생 패턴에 대한 통계 데이터 중 낮은 발생 회수를 보이는 요청 형태에 대한 이력을 기록한 후 다음과 같은 특징에 대한 화이트 리스트 작성을 수행한다.

(i) 일정기간 동안 부분 사용자 그룹에 의하여 동일하게 나타나는 비정형 데이터 요청은 악성코드의 배포 또는 공격의 확률이 높다.
(ii) U-city 센서 통신의 경우 비정형 데이터의 송수신이 발생할 확률이 낮다.

6. 예·경보 이용 통계 데이터

이용 통계 학습은 앞서 제시된 알고리즘에 적용하기 위한 기초 통계자료로 다음과 같은 규칙에 의하여 생성 된다.

(i) 타임 슬롯으로 구분되는 통계 데이터 생성
(ii) DNS이용 분석을 위한 데이터
- 질의 URL
- 요청자 IP
- 응답 IP
(iii) 통신 분석을 위한 데이터
- 출발지 IP, Port, MAC
- 목적지 IP, Port, MAC
- Protocol
(iv)TCP 분석을 위한 데이터
- Sequency Number
- Control Bit
(v) 요청 분석을 위한 데이터
- TCP Data Hash code

III. 예·경보 오차범위 보정 알고리즘

예·경보 알고리즘에 의하여 생성된 화이트 리스트를 이용한 오차범위 보정 알고리즘은 신뢰성 있는 예·경보 데이터의 생산을 위하여 사용된다.

오차 범위 보정은 동일한 보정 규칙의 적용을 개별 U-city의 화이트 리스트를 모집단으로 수행 것과, 복수의 U-city 생성 화이트 리스트를 이용한 반복 연산을 수행하는 방식으로 구분 된다.

화이트 리스트는 다음과 같은 순서에 의하여 블랙리스트로 전환 되는 과정을 수행한다.

(i) U-City내의 이용자 IP 그룹을 실제 네트워크 구성 단위로 그룹화 한다.
(ii) 개별 그룹에서 생성된 화이트 리스트와 검출 패턴을 타 그룹과 비교 한다.
(iii) 생성 데이터의 신뢰도를 운영자가 분석하여 임계치를 보정함으로서 블랙리스트 생성의 신뢰 구간을 형성한다.

개별 네트워크 그룹에서 발생한 화이트 리스트는 다음의 규칙을 적용하여 블랙리스트로 전환됨으로서 오차 범위를 보정 한다.

(i) 신규 URL(IP) 요청 발생 범위가 지역적으로 발생
(ii) 주기적 URL(IP) 요청 발생 범위가 지역적으로 발생
(iii) URL 이 할당되지 않은 IP로의 사용자 접속이 낮은 분포의 IP에서 발생.
(iv) 특정 서비스에 대한 요청이 낮은 분포의 IP로부터 높은 빈도로 발생
(v) 단기 이용 후 소멸되는 URL(IP)의 재 발생 패턴 및 발생 범위가 지역적, 순차적으로 발생
(vi) 복수 지역 사용자의 특정 서비스 이용 요청 급증이 낮은 분포도로 발생
(vii) 특정 비정형 데이터 요청이 복수 지역 이용자에게 높은 분포도로 발생
(viii) 유사 규모의 네트워크 통신이 통계 수치 이상으로 검출
(ix) 유사 규모의 외부 네트워크 사용 통신이 통계 수치 이상으로 검출

이와 같은 규칙에 의하여 생성된 블랙리스트는 예·경보 데이터로 사용하게 된다.

IV. 공격 근원지 및 감염 예상 PC 추적 알고리즘

공격 근원지 및 감염 예상 PC 추적 알고리즘은 공격 행위의 예측 또는 발생을 통하여 획득한 데이터를 기준으로 하여 추적하는 것을 원칙으로 한다.

공격에 가담한 IP는 악성코드의 감염 또는 C&C 서버로의 접속을 위하여 동일한 IP 또는 URL에 접속한 이력을 갖게 된다. 여기서 동일한 IP 또는 URL은 특정 IP, URL로 지정되는 경우도 있으나 복수의 IP 또는 URL로 산포되어 나타나는 경우가 일반적이다.

이러한 다양한 감염 정로를 추적하기 위하여 공격에 참여한 개별 IP들이 접속한 URL 목록 중 중복 되는 IP 목록의 중복 확률을 연산 방식으로 공격 근원지 목록을 생산 한다.

감염 예상 PC 추적은 공격에 가담하지 않았으나 공격 근원지 목록의 URL 또는 IP에 접속한 이력을 보유한 PC을 추적함으로서 수행된다.

상기 과정을 반복적으로 수행하여 감염 예상 PC를 이용한 제2의 공격 근원지 목록을 예측 하고,이를 이용하여 다시 감염 예상 PC의 추적을 실행 하게 된다.

V. 피해 예상 규모 추정 및 파급 경로 분석

피해 예상 규모의 추정은 감염 예상 PC 예측을 통하여 실현된다. 감염 예상 PC는 공격에 동원 되는 좀비 PC의 숫자와 동일하게 산출 되므로 특정 서비스에 대한 공격 예상 규모로 대입 된다..

파급 경로 분석은 특정 지역에서 나타난 감염 예상 PC을 발생 시간 별로 추적 하여 특정 U-city에서 타 U-city로 분포 확산 되어 가는 과정을 분석 하게 된다.

파급 경로는 지역적 경로의 특성을 가질 수도 있지만 사이버 공간의 특징상 특정 이용 경향을 가진 사용자 그룹이라는 가상의 경로를 산정하게 된다.

공격자는 자신의 악성코드를 확산하기 위하여 보안이 취약한 특정 서비스 서버를 공격하고, 이를 이용한 악성코드 유포를 실시한다. 2009년 7월 7일 발생한 DDos 공격의 경우 특정 회사의 웹하드 서비스 공격을 통한 악성코드 유포 및 공격 시행이 대표적인 가상 경로로 규정 할 수 있다.

VI. 결 론

본 논문은 사이버 테러 방지를 위한 예·경보 알고리즘의 적용을 위하여 복수 네트워크의 집합체인 U-City를 대상으로 하는 통계적 예측 및 추적 기법을 제안하였다. 단일 네트워크에서의 통계 측정 또는 내부 네트워크 통신 모니터링에 의한 분석은 개별 네트워크 보안의 향상을 가져 올 수 있으나 개별 네트워크 단위에서 타 네트워크로 발생하는 공격에 대한 해결 방안이 되지 못하였다. 제안 하는 예·경보 알고리즘은 복수 네트워크에서의 공격 및 피해를 사전에 탐지하여 개별 네트워크의 방어를 위한 데이터로 재사용 하여, 개별 네트워크 보안 효율을 높이고 전체 네트워크의 위협을 차단하는 효과를 제공 할 수 있다.

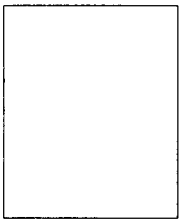
감사의 글

이 연구을 위하여 기초 자료 및 데이터 수집을 위하여 노력하여 주신 김용진, 김욱진, 오종현, 정윤교, 윤경식 님에게 감사의 글을 남깁니다.

[참 고 문 헌]

[1] 이범교, 김현주, 한진우, "U방재city서비스 및 기술에 관한 연구", 정보통신설비 학술대회, pp. 277~280, 2008.

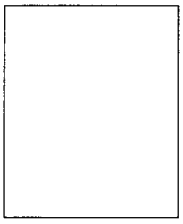
[2] 이규환, 김재현, "RFID시스템에서DoS공격을 포함한 다양한 공격에 대처하는 인증기법", 정보통신설비 학술대회, pp. 146~149, 2008.



김 형 중

1978년 서울대학교 전기공학과(학사)
1986년 서울대학교 제어계측공학과(공학석사)
1989년 서울대학교 제어계측공학과(공학박사)
1989년~2006년 강원대학교 교수
2006년~ 현재 고려대학교 교수

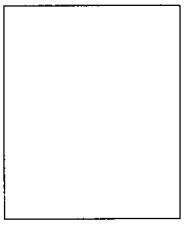
<관심분야> 센스네트워크, 최적화, 신호처리,분산처리, 컨텐츠공학
<e-mail>khj@korea.ac.kr



정 규 일

1982년 동양공업대학 전기공학과 졸업
1987년 숭실대학교 전자공학과(공학석사)
2007년 ~ 경희대학교 스포츠의학과(박사)
2005년 ~현재 (주)에이원테크,연구소장

<관심분야> 센서네트워크, 네트워크보안,다중영역구분보안, 신호처리, 유,무선U-헬스케어시스템, 유,무선U-ecoland city산업화, 유,무선U-farm마을산업화,광가입자망(FTTH)구성기술연구
<e-mail> kyouil@paran.com



이 준 엽

1996년 서울산업대학교 전기공학과 4년 재적
2003년 (주)케이게이트 기반기술연구소 소장
2009년 현재 (주)시큐에버 R&D 사업부
<관심분야> 다중영역구분보안,
네트워크 보안, 네트워크 패킷 통계 분석
<e-mail> jylee@secuever.com