SDN을 이용한 사이버 검역 시스템 설계

김남욱*, 정준권*, 송영배**, 김형식***, 정태명***
* **성균관대학교 전자전기컴퓨터공학과
***성균관대학교 정보통신대학

e-mail: *{nukim, jkjung}@imtl.skku.ac.kr, **usa3234@naver.com
***{hyoung, tmchung}@skku.edu

The Design of SDN Quarantined Network

Nam-Uk Kim*, Jun-Kwon Jung*, Youngbae Song*, Hyoungshick Kim**,
Tai-Myoiung Chung**
*Dept of Electrical and Computer Engineering, SungKyunKwan University
**College of Information and Computer Engineering, SungKyunKwan University

요 약

기존 보안 기술들은 기관 내부 망을 이루는 각각의 영역에 대해 이미 알려진 공격에 대한 방어에서는 강점을 가진다. 하지만 공격자가 다양한 제로데이 공격 기술과 사회공학적 기법을 적절히 활용하여 공격할 경우, 기존 기술만 이용하여 이를 방어하기는 매우 어려운 실정이다. 더 이상 개별적인 방어 방식으로는 고도화된 공격을 막을 수 없게 되었다. 이에 통합 관제에 적합한 솔루션이 등장하고 있지만, 현재는 단지 각 솔루션에 대한 통합 관리 기능에 국한되어 있을 뿐이다. 이에 본 논문에서는 체계적이고 통합적으로 기관 내부망을 청정하게 유지할 수 있는 새로운 형식의 보안 시스템을 제안하였다.

1. 서 론

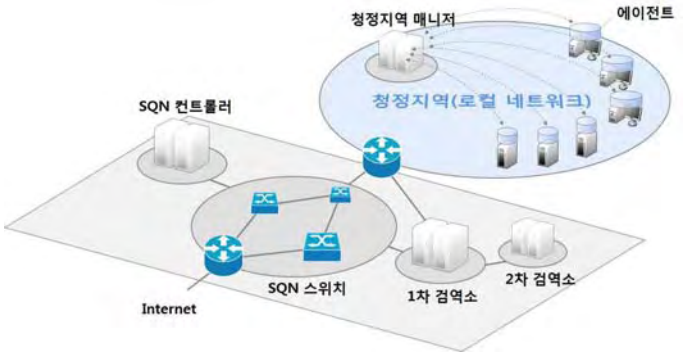
사회와 경제를 이루는 거의 모든 부문에서 정보화 시스템의 의존도가 증대하면서, 정보보호에 대한 문제도 끊임없이 제기 되고 있다. 특히 요즈음에는 각종 정보보호 솔루션이 존재함에도 불구하고 정보침해사고가 끊임없이 발생하고 있으며, 오히려 피해 규모는 범국가적인 대응이 필요할 만큼 심각해지고 있다. 최근 몇 년 사이에는 사이버 공격의 양상이 급변하여 치밀한 계획 하에 고도화된 기술을 활용하여 특정 시스템 및 내부 정보를 노리는 형태의 공격이 급증하였다.

기존 보안 기술들은 기관 내부 망을 이루는 각각의 영역에 대해 이미 알려진 공격에 대한 방어에서는 강점을 가진다. 하지만 공격자가 다양한 제로데이 공격 기술과 사회공학적 기법을 적절히 활용하여 공격할 경우, 기존 기술만 이용하여 이를 방어하기는 매우 어려운 실정이다. 더 이상 개별적인 방어 방식으로는 고도화된 공격을 막을 수 없게 되었다. 이에 통합 관제에 적합한 솔루션이 등장하고 있지만, 현재는 단지 각 솔루션에 대한 통합 관리 기능에 국한되어 있을 뿐이다.

이에 본 논문에서는 체계적이고 통합적으로 기관 내부 망을 청정하게 유지할 수 있는 새로운 형식의 보안 시스템을 제안하고자 한다.

2. 사이버 검역 시스템의 구성

본 논문에서 제안하는 사이버 검역 시스템의 전체적인 구성은 다음 그림과 같다.



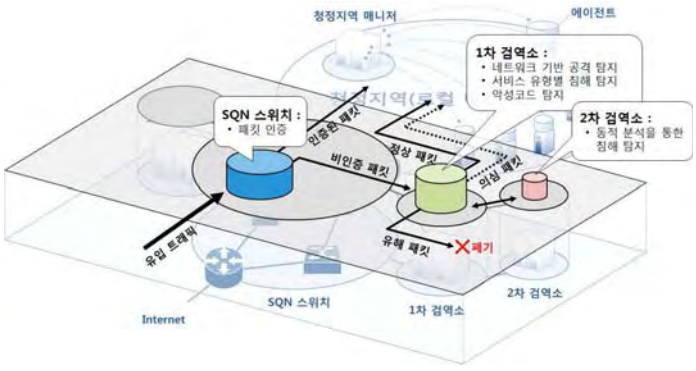
(그림 1) 사이버 검역 시스템 구성

보호하고자하는 로컬 네트워크로 유입되는 패킷을 검역하기 위하여 SQN(SDN Quarantined Network) 스위치, SQN 컨트롤러, 1차 검역소, 2차 검역소가 협력하여 동작한다. SQN 스위치와 SQN 컨트롤러는 SDN 스위치와 SDN 컨트롤러를 본 시스템의 목적에 부합하도록 수정한 것이라 보면 된다.

또한 로컬 네트워크 내부에서는 해당 네트워크를 청정지역으로 유지하기 위하여 모든 시스템에 에이전트가 배치되고, 이들은 청정지역 매니저를 통해 통합 관리된다.

3. 사이버 검역 시스템의 주요 기능

사이버 검역 시스템의 기능은 크게 유입 패킷에 대한 검역 기능과 내부 네트워크의 청정 유지 기능으로 나뉜다. 유입 패킷 검역 과정은 다음 그림과 같다.



(그림 2) 유입 패킷 검역 과정

본 논문에서 제안하는 사이버 검역 시스템의 가장 큰 특징 중 하나는, 인증된 패킷에 대해서는 검역 절차 없이 바로 로컬 네트워크로 전달함으로써, 검역에 따른 시스템 부하를 최소화하는 것이다. SQN 스위치와 SQN 컨트롤러는 이러한 패킷 인증을 수행하기 위하여 존재한다. 또 다른 사이버 검역 기반 네트워크에서 패킷을 전송할 때 해당 패킷에 대한 인증 태그를 첨가하여 전송하는데, SQN 스위치와 SQN 컨트롤러는 패킷에 대한 인증 태그를 확인하여 안전성을 확신하게 된다. 이러한 절차를 패킷 인증이라 지칭한다.

인증되지 않은 패킷에 대하여는 1차 검역소에서 다양한 방식으로 공격을 탐지하게 되며, 탐지 결과를 정상, 의심, 유해로 나누어 처리한다. 정상일 경우 바로 로컬 네트워크로 전송하며 의심일 경우에는 의심 태그를 부착하여 전송한다. 유해일 경우에는 로그를 남긴 후 폐기한다.

2차 검역소는 첨부파일이 있는 트래픽에 대하여 에뮬레이션을 이용한 동적 분석을 통해 공격을 탐지하기 위한 시스템으로, 1차 검역소에서 탐지하지 못한 공격을 다소 시간이 걸리더라도 탐지해 내기 위해 존재 한다.

검역을 통해 의심 판정을 받은 패킷이 로컬 네트워크에 있는 특정 시스템 내부로 들어갔을 경우, 해당 시스템의 감시 에이전트에서는 그 패킷과 관련된 프로세스를 의심 프로세스로 지정하고 행동을 감시한다. 특정 프로세스가 민감 정보에 접근할 경우에도 마찬가지로 해당 프로세스의 행동을 감시한다. 이러한 감시는 보안 정책에 따라 이루어지며, 보안 정책에 위배된 행위가 발생하였을 경우, 이벤트를 청정지역 매니저에게 전송하여 알린다.

(그림 3) 로컬네트워크 청정 유지 기능

청정지역 매니저는 크게 에이전트 관리 기능, 이벤트 관리 기능, 정책 관리 기능을 가지는데, 에이전트 관리 기능은 네트워크 내 에이전트 추가, 삭제, 배치 등 구성 관리와, 에이전트에 대한 인증 기능을 지칭한다.

감시 에이전트로부터 수신한 이벤트는 총체적인 분석을 통하여 또 다른 공격을 탐지할 수 있고, 새로운 정책을 자동으로 설정하는데 사용될 수 있다. 이벤트 관리 기능이 이러한 역할을 수행한다.

보안 관리자는 정책 관리 기능을 통해 각 에이전트에 전달될 보안 정책을 관리할 수 있다.

4. 결 론

본 시스템은 개별적인 방어 위주의 기존 보안 방식의 틀에서 벗어나 통제 위주의 새로운 보안 방식을 적용함으로써, 고도화되고 예측하기 힘든 공격을 방어할 수 있는 새로운 보안 패러다임을 제시한다. 앞으로 본 시스템을 이루는 각 컴포넌트에 요구되는 세부적인 기술에 대한 연구를 지속할 것이다.

ACKNOWLEDGEMENT

본 연구는 미래창조과학부가 지원한 2014년 정보통신·방송(ICT) 기술개발사업의 연구결과로 수행되었음[SDN 기술을 이용한 사이버 검역 시스템 개발]

참고문헌

[1] Tankard, Colin. "Advanced Persistent threats and how to monitor and deter them." Network security 2011.8 (2011): 16-19.

[2] McKeown, Nick. "Software-defined networking." INFOCOM keynote talk (2009).