IoT 환경에서의 악성패킷 탐지 솔루션 모델 구축 제안

서초롱*, 양희탁*, 이근호*, 전유부**
*백석대학교 정보통신학부
**순천향대학교 컴퓨터소프트웨어공학과 & 웰니스코칭서비스연구센터
e-mail:dndbtnr222@naver.com, satelpial@gmail.com, root1004@bu.ac.kr, jeonyb@sch.ac.kr

Propose to malicious-packet detection solution in the IoT

Cho-Rong Seo*, Hee-Tak Yang*, Keun-Ho Lee*
*Division of Information and Communication, Baek-Seok University
**Computer Software Engineering & Wellness Coaching Services Research Center, Soon-Chun-Hyang University

요 약

최근 IT 기술이 눈에 띄게 발전해 가고 있는 가운데 그 중에서도 사물인터넷 또한 많은 발전을 해오고 있다. 그러나 사물인터넷은 보안에 매우 취약한 단점이 있다. 그 중에서도 요즈음 사물인터넷을 대상으로 한 랜섬웨어 공격이 기승을 부린다고 전해진다. 그 중 웹에 접속하여 파일을 다운받는 경로가 가장 많이 감염되는 경우이다. 이처럼 사용자가 원치 않게 악성코드가 다운되는 경우가 급격히 증가하고 있다. 본 논문에서는 이러한 경우를 고려하여 IoT 기기를 통해 파일을 다운 받거나 위험성이 있는 사이트에 방문 시 빅데이터를 사용하여 데이터를 먼저 분석하여 위험성 있는 구문을 삭제하거나 차단하여 안전한 데이터들만 사용자에게 전송하는 프로그램을 만들어 사용자의 디바이스를 보호하는 방향을 제안한다.

1. 서론

IT의 발전으로 많은 악성코드가 퍼지고 있으며, 요즈음 대표적인 악성코드로는 랜섬웨어로서 매년 2배 이상 씩 증가하며 기승을 부리고 있다. 2013년에서 2014년 사이 악성코드로 인한 공격이 2배 이상 증가했으며 2016년에는 전년도보다 5배 이상 증가하는 등 매년 수가 증가하고 있다. IT전문가들은 2020년에는 지금보다 18배 이상 증가할 것으로 내다보고 있다. 감염경로는 이메일이 23%가 넘으며 웹의 접속으로 다운받아지는 경우는 34%에 가 넘을 정도로 많은 비중을 차지하고 있다. 웹의 경우 인증서나 방화벽으로 사용자를 보호하고 있지만 일부인 37%를 막을 수 있다. 이는 나머지 위험한 사이트에는 접속을 해도 사용자는 모른다는 것이다. 특히 IoT기기는 더욱 심각할 것이다. 매년 IoT기기는 증가하고 있으며 2021년에 IoT환경과 연결된 사물이 230억 개가 넘어 갈 것으로 전망하고 있다. 더불어 사용자가 원치 않아도 검증되지 않은 사이트에 들어가지는 경우도 빈번히 발생하는 만큼 사용자가 원치 않아도 접속되어 악성코드가 다운되는 경우가 증가한다. 웹사이트의 서버 또는 데이터베이스를 관리하는 곳의 취약점 때문에 발생할 가능성이 가장 크지만 이로 인해 크래커들에게 피해를 보는 것은 사용자로 돌아간다. 이 개인정보는 스피어피싱로 이용이 될 가능성이 높으며 이것은 2차, 3차의 피해를 유발한다. 그러므로 사용자 또한 이에 대해 보호할 수 있는 백신 프로그램과 같은 프로그램이 필요성 있다 크게 예측이 된다. 사용자의 주의도 필요하지만 IT의 급성장적인 발전으로 대응하기 위해서는 사용자를 웹으로부터 추가적으로 보호하는 백신 프로그램의 필요성 또한 배재할 수 없다. 또한 IoT의 경우 많은 기기들이 웹사이트를 통해 관리 및 사용하는 경우가 많기에 이것을 악의적으로 이용하여 공격하는 경우가 있기 때문에 보호차원에서 많은 필요성이 예측된다. 위 논문은 그러한 악의적인 웹사이트로부터 IoT기기의 정보를 사전에 보호할 수 있도록 하는 프로그램을 구상한다.

2. 관련연구

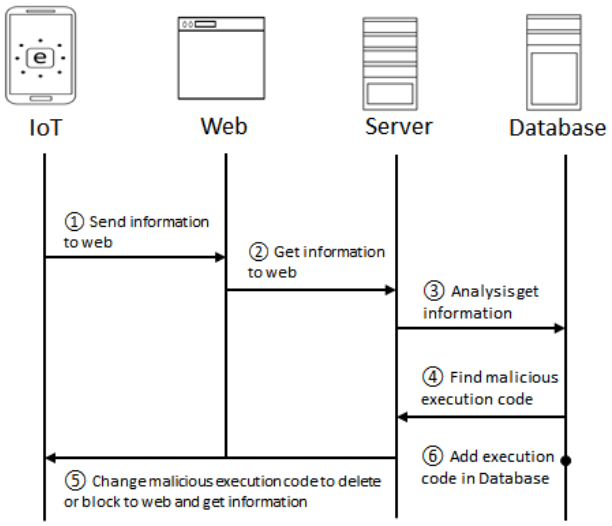
2.1 Burp Suite

Burp suite는 사용자의 컴퓨터와 네트워크를 통해 웹 서버로 주고받는 패킷을 사용자가 보내기 전 패킷과 사용자가 받아 실행시키기 전 패킷을 잡아서 확인, 수정을 할 수 있는 대표적인 패킷탐지 프로그램이다. 네트워크의 포트를 지정하여 그 포트에서 움직이는 정보를 캡쳐한 후 나가지 못하도록 막는 원리이며, 받는 것 또한 같은 원리이다. 취약점 분석 및 웹 페이지 분석으로 널리 사용된다. 위 논문에서 제시하는 방향은 Burp suite의 기능 중 패킷을 변경이 아닌 응답 패킷에 대한 구문분석이다. Burp suite를 이용해 응답 패킷을 변경하는 원리가 아닌 포트를 지정해 분석서버로 응답패킷을 분석한 뒤 사용자로 오는 방향으로 구상한다.

2.2 빅 데이터

기업 또는 개인적인 업무와 관련된 운용 설비 또는 데이터로부터 생성되는 로그 데이터 등 오늘 날 개인 또는 기업이 하루에 처리해야하는 정보의 양이 날이 갈수록 늘고 있다. 이러한 문제점을 해결하기 위하여 최근 IT 기술은 소프트웨어, 네트워크, 하드웨어 관련 서비스 등 각종 분야에서 혁신적인 발전을 거듭하여 생성 된 것이 빅 데이터다[1,2,3]. 이러한 빅 데이터를 본 논문에서는 프로그램이 분석한 데이터를 기존에 있던 데이터베이스의 데이터 내용과 비교하여 다를 경우 신뢰를 얻지 못한 부분을 제거 또는 차단하는 과정에서 새로 들어온 데이터를 비교할 기존의 데이터들을 저장해 두는 공간으로 지정한다. 데이터의 경우 이미 있는 유형에서 약간씩 변경이 되어 공격됨에 따라 같은 분류끼리 묶고 비슷한 것은 연결시켜 묶는 이명법 형식으로 연결시켜 나열시킨다. 이를 키워드로 통하여 1차 나열과 2차 나열로 세부적으로 검색해 접근, 같은 연관성 분석 및 다른 부분 3차 분석을 하여 추가나열을 통해 데이터 내용을 찾는다. 이때 3차에 비슷한 내용이 없을 경우 그 내용들을 다른 내용들과 한 단어씩 대입, 분석하여 새로운 결과 값을 도출하고, 데이터를 업데이트 시킨다.

3. 제안사항



(그림 1) 프로그램 시나리오

① 사용자가 웹페이지에 접속하며 웹 페이지에 대한 정보를 요구하는 패킷을 보낸다.
② 웹 페이지는 패킷을 사용자에게 보내는 것이 아니라 분석하는 서버로 보낸다.
③ 서버는 데이터베이스에 있는 자료들을 이용해 분석한다. 이때 이진명법으로 데이터화되어있는 데이터를 이용하고 데이터에 없는 내용은 다른 데이터와 한 단어씩 대입, 새로운 값을 도출시킨다.
④ 데이터베이스는 악성코드를 찾는다.
⑤ 사용자로 보낼 때 악성코드를 삭제하거나 웹을 블록 시켜 피해를 없앤다.
⑥ ③에서 분석한 내용을 이진명법으로 추가 업데이트를 시킨다.

4. 결론

요즈음 정보통신 기술들이 눈에 띄게 발전해 가고 있는 가운데 그 중 사람들과 밀접하게 연관되어 있는 분야인 사물인터넷이 최근 랜섬웨어의 공격을 많이 받고 있다고 전해진다. 이처럼 예전부터 사물인터넷의 보안은 매우 취약한 것으로 알려져 있다. 랜섬웨어 뿐만 아니라 다운로드를 통한 감염과 이메일을 통한 감염도 높은 비중을 차지하고 있다. 또한 이러한 감염으로 인하여 본인이 원치 않게 검증되지 않은 사이트에 들어가 안전하지 않은 파일을 다운로드 함으로써 2차로 감염되는 경우도 빈번히 발생하고 있다. 이러한 사물인터넷의 취약한 보안적인 문제점을 보안하고자 본 논문에서는 사이트로부터 사용자를 사전에 보호 할 수 있도록 하는 프로그램을 만들어 IoT 환경에서 사용자들을 보호하는 방안을 제시한다. 먼저, 사용자들은 해당 프로그램을 사용 디바이스에 설치를 한다. 사용자가 웹 페이지에 접속을 하여 웹 페이지에 대한 정보를 요구하는 패킷을 보낸다. 그런 후 웹 페이지는 패킷을 사용자에게 보내지 않고 본 논문에서 제안한 프로그램으로 전송하여 데이터베이스에 있는 자료들과 비교한다. 이때 만약 비교하는 과정에서 악성코드 또는 안전하지 않은 정보를 발견 할 경우 차단시키거나 악성코드를 삭제하여 사용자에게 보낸다. 이럴 경우 사용자들이 의도치 않게 감염 경로로 들어갔을 때 생기는 감염으로부터 예방할 수 있다.

감사의 글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음(IITP-2016-H8601-16-1009). 또한 2016년 산학협동재단 지원으로 수행된 연구임.

참고문헌

[1] Hwan-soon Lee, Dong-Won Lim, Hang-Jung Zo, "Personal Information Overload and User Resistance in the Big Data Age", Korea Intelligent Information Systems Society, Vol. 19, No. 1, pp. 125-139, 2013.
[2] Won-Jin Lee, In-Gyu Lee, Byung-Won On, Jung-In Choi, "A Study on Big Data System to Analyze Smart Grid Energy Data", Korea Information Science Society, Vol. 32, No. 9, pp. 35-41, 2014.
[3] Kwang-Il Kim, Jung-Sik Jeong, Gyei-Kark Park, "Assessment of External Force Acting on Ship Using Big Data in Maritime Traffic", Korea Institut of Intelligent Systems, Vol. 23, No. 5, pp. 379-384, 2013.