보안성이 검증된 소프트웨어 등록·활용 시스템 구축을 통한 정보보안 강화 방안

여 동 균* 공 병 철** 이 근 혁***

◈ 목 차 ◈

1. 서 론

최근 은행이나 기업에서 사용하는 보안솔루션 및 편의상 사용하는 유틸리티 프로그램의 취약한 사항을 이용하여 사이버공격이 이루어지는 경우가 비일비재하다.

가장 큰 피해를 입은 침해사고는 2013년 3.20사이버 대란 때 백신서버의 중앙패치관리시스템의 무결성 검증을 수행하지 않아 동시에 수많은 단말기로 악성코드를 전파한 사례가 있었다. 2016년 백신 중계서버 및 중앙관리서버 등의 허점을 이용하여 수많은 에이전트가 설치된 단말기로 악성코드를 감염시킨 사례가 최근까지도 빈번히 발생하고 있다.

이처럼 소프트웨어의 취약점을 이용한 공격은 지능화 고도화로 증가함은 물론이며, 국가적 대형 침해사고의 피해를 일으키고 있는 실정이다. 하지만 소프트웨어의 규모나 용도에 상관없이 개발된 소프트웨어에 대해 검증하는 절차나 등록하는 과정 등의 인증체계가 국내에서는 미흡한 실정이다. 이러한 이유로 본 논문에서는 보안성이 검증된 소프트웨어 등록·활용 시스템 구축을 통한 정보보안 강화 방안에 대하여 연구하였다.

* (주)이글루시큐리티
** (사)한국사이버감시단
*** (사)한국정보통신진흥협회

2. 다양한 소프트웨어 인증 실태

2.1 소프트웨어 품질 인증 관련 법률

국내에서는 다양한 소프트웨어 품질 확보 및 유통 촉진을 위하여 소프트웨어에 관한 품질 인증을 실시할 수 있다는 것을 '소프트웨어산업진흥법'에서 명시하고 있다.

제13조(품질인증) ① 미래창조과학부장관은 소프트웨어의 품질 확보 및 유통 촉진을 위하여 소프트웨어에 관한 품질인증을 실시할 수 있다.
② 미래창조과학부장관은 제1항에 따른 품질인증을 실시하기 위하여 인증기관을 지정할 수 있다.
③ 제2항에 따라 지정받은 인증기관은 소프트웨어 품질인증의 신청을 받은 경우 대통령령으로 정하는 인증기준에 맞다고 인정하면 품질인증을 하여야 한다.
④ 미래창조과학부장관은 제1항에 따라 품질인증을 받은 제품에 대하여 「중소기업제품 구매촉진 및 판로지원에 관한 법률」 제13조에 따른 공공기관의 우선구매 및 「기초연구진흥 및 기술개발지원에 관한 법률」 제4조에 따른 자금지원 등을 중앙행정기관의 장에게 요청할 수 있다.
⑤ 미래창조과학부장관은 제2항에 따라 인증기관으로 지정받은 자가 다음 각 호의 어느 하나에 해당하게 된 때에는 그 지정을 취소할 수 있다.
1. 거짓이나 그 밖의 부정한 방법으로 지정받은 경우
2. 대통령령으로 정하는 지정 요건에 계속하여 3개월 이상 미달한 경우
3. 인증기준에 맞지 아니한 제품에 대하여 품질인증을 한 경우
⑥ 제2항에 따른 인증기관의 지정 요건 등 소프트웨어 품질인증의 실시에 필요한 사항은 대통령령으로 정한다.

2.2 소프트웨어 인증 현황

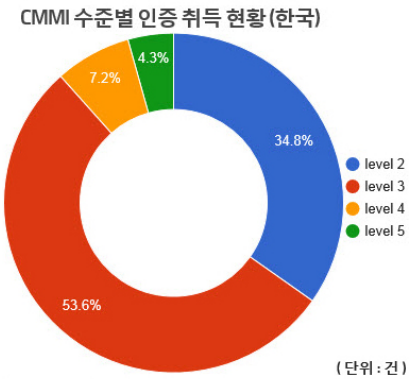
국내 및 해외의 각종 소프트웨어와 관련한 인증이 다수 존재한다. 인증의 종류로는 대표적인 GS 인증 외에 아래와 같이 다양하다.

(표 1) 국내외 소프트웨어 인증내용

NO	종 류	인증내용	활용 국가	비 고
1	GS	SW제품에 대한 인증	한국	SW제품이 제대로 작동하는지에 대한검증
2	TMMI	SW 테스트 프로세스 인증	국제	테스트 성숙도에 대한 인증
3	CMMI	SW 프로세스 인증	국제	개발 프로세스 성숙도에 대한 기업 인증으로 미국을 중심으로 널리 사용되고 있음
4	ISO 9001	품질경영시스템에 대한 인증	국제	ISO에서 제정한 품질경영시스템에 관한 국제규격 인증. 세계적으로 인정받는 품질경영 체제로 품질경영시스템 뿐만 아니라 일반 경영시스템까지 포괄함.
5	SPICE	SW 프로세스 인증	국제	개발 프로세스에 관한 인증으로 유럽을 중심으로 널리 사용되고 있음
6	SP	SW 프로세스 인증	한국	SW 개발 프로세스에 관한 기업 인증
7	CC	보안적합성 인증	한국	정보보호시스템 보안적합성 인증
8	웹접근성 품질마크	웹사이트 접근성 인증	한국	장애인 및 고령자가 웹 사이트 사용함이 용이한지 확인하는 인증
9	TMMi	SW 프로세스 인증	국제	SW테스팅 프로세스의 성숙도를 점검하고 개선방향을 가이드하는 모델

그러나 유독 보안성 검증을 통한 인증은 보이지 않는다.

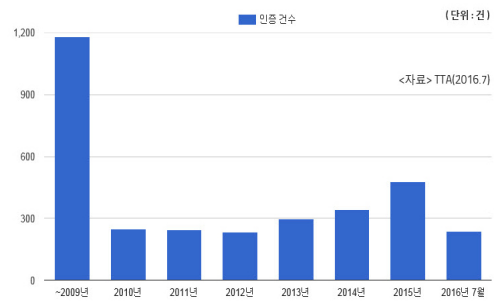
(그림 1) 소프트웨어 인증 마크



(단위 : 건)

국가	level 2	level 3	level 4	level 5
한국	72	111	15	9

(그림 2) 국내 CMMI 인증 취득현황



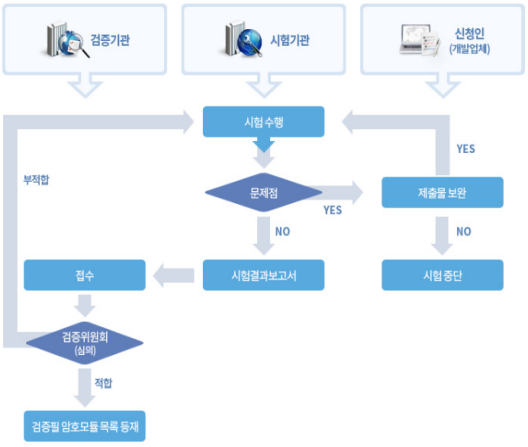
구분	~2009년	2010년	2011년	2012년	2013년	2014년	2015년	2016년 7월	누적합계
인증 건수	1,182	248	245	233	299	342	476	237	3,262

(그림 3) 국내 GS 인증 취득현황

3. 소프트웨어 보안성 검증 사례

3.1 국내 공공기관의 보안성 검증 사례

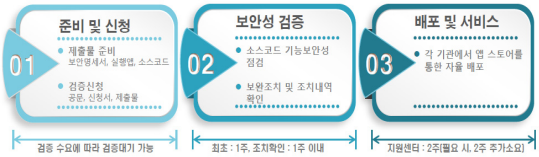
공공기관에서는 암호화 소프트웨어 제품에 대하여 소스코드 등의 보안성 검증을 수행하는 국정원의 암호모듈 인증이 있다.



(그림 4) ETRI 암호모듈 시험 및 검증 절차

2015년 1월 부터는 모든 공공기관의 전자정부사업중 20억원 이상의 웹 응용프로그램(홈페이지, 소프트웨어 등) 개발, 구축시에는 시큐어 코딩 적용 여부에 대한 검증을 의무화 하고 있다.

또한 웹 응용프로그램 뿐만 아니라 개발 규모에 상관없이 대국민 서비스용의 모바일 앱에 대해서도 소스코드 보안성을 의무적으로 검증하고 있다. 단 행정기관 및 공공기관의 모바일 대민서비스 구축시에만 개발 보안 적용을 의무화 하고 있어, 일반적인 모바일 앱의 보안성은 보완되지 않고 있다.



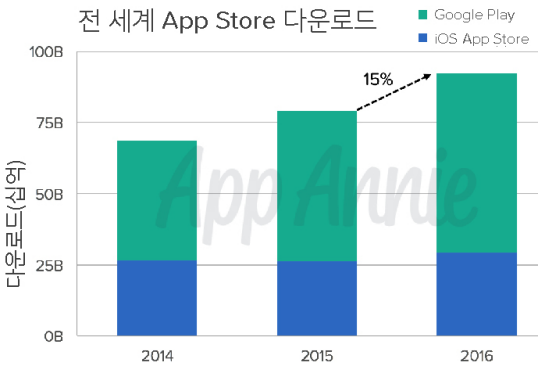
(그림 5) 모바일 대국민 전자서비스 앱 소스코드 검증 체계

또한 모바일 용의 앱(APP)을 개발하여 업로드시에 통신사의 앱 마켓 및 다운로드 사이트 등에서는 악의적인 행위를 하는 앱인지 검증을 하고 있다.

해외의 구글 플레이 스토어 등과 같은 앱 다운로드 사이트에서도 기본적으로 악성 앱을 차단하는 검증을 수행하고 있다. 그러나 모든 개발된 소프트웨어 대해 안정성 검증을 거치지 않고 업로드가 가능한 사이트가 수없이 많이 존재하며, 무분별하게 인터넷을 통해 전파되는 상황이다. 해외 사이트 중에서 '바이러스토탈(www.virustotal.com)'에서는 파일, URL등에 대한 악성코드 존재 여부를 검증하고 있다. 따라서 컴퓨터 및 핸드폰 또는 IoT(사물인터넷) 단말기 등 미래 지능정보사회의 다양한 스마트디바이스 장비에서 사용되는 응용소프트웨어의 안정성을 강화하기 위해서는 이를 검증하는 효율적인 체계가 필요하다.

3.2 국내 통신사 모바일 마켓 운영 사례

2016년 전 세계 iOS App Store와 Google Play를 합쳐 연간 다운로드가 130억 건 넘게 증가하면서 900억 건을 돌파했다.



(그림 6) 2016년 전 세계 App Store 다운로드수

국내 모바일용 앱을 다운로드 할 수 있는 앱 마켓은 통신사 전용마켓이나 포털(네이버) 등에서 제공하고 있으며, 안드로이드 앱 마켓 시장은 구글의 플레이스토어 75%, SK텔레콤 T스토어 8%, 네이버 앱스토어 8%, KT 올레마켓 4%, LG유플러스 U+스토어 4% 등의 시장점유율을 보이고 있다.

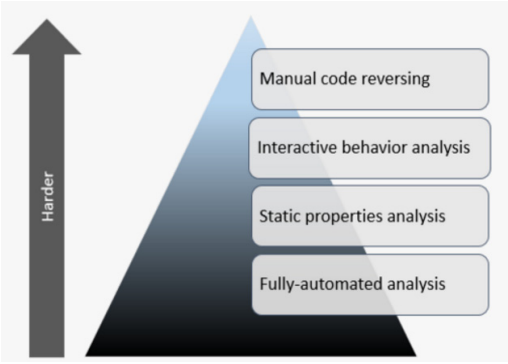
지난 2016년 6월 통신 4사 통합 앱마켓 '원스토어' 서비스가 시작되었다. 원스토어 사업에 참여하는 통신사업자들과 인터넷사업자 간의 시너지를 통해 앱, 게임, 전자서적, 음악, VOD 등 모든 디지털 콘텐츠는 물론 휴대폰 액세서리 쇼핑까지 한곳에서 즐길 수 있는 서비스이다.

4. 소프트웨어 보안성 검증 방법

소프트웨어에 대한 보안성 검증은 크게 보면 두 가지 측면에서 살펴볼 수 있다.

첫 번째는 소스코드를 검증하여 보안취약점이 존재하는지에 대한 정적분석으로 검증하는 방법이다.

두 번째는 소스코드 검증이 아닌 단순히 프로그램내에 악성코드가 포함되어 있는지를 동적분석으로 검증하는 방법이다.



(그림 7) 악성코드 분석 방법 4가지

위 정적분석과 동적분석 두 가지 방법이외에 상세분석방법에 대한 사항을 살펴보자.

첫째, 완전 자동화된 분석(Fully-automated analysis)방식이다.

하루에도 수 만개씩 쏟아지는 악성코드를 전문 분석가들이 하나씩 분석할 수는 없는 일이다. 악성코드의 정적분석 및 동적 분석을 통한 악의적인 행위를 판단할 수 있을 정도의 분석을 위해 자동 분석의 활용은 꼭 필요하다. 물론, 이런 분석들안에 포함되는 파일생성, 수정 과정의 분석, 레지스트리 분석, 네트워크 분석 등이 전문가에 의해서 하나씩 분석되는 과정만큼 상세하거나 정확하지 않을 수 있다. 따라서 악성코드 분석을 위한 도구 툴들과 악성코드 분석 제공 서비스들이 해당된다.

둘째, 정적 속성 분석(Static properties analysis)방식이다.

실행 파일의 문자열 헤더 정보, 해시값, 리소스 정보, 패킹여부 등 신속하게 획득할 수 있는 정보는 악성코드의 추가 분석을 위한 필요한 단계이다. 이러한 정보들은 실행파일간의 비교 데이터베이스를 구성하는데도 간단하게 활용할 수 있다. 정적분석 사례, XOR 난독화 분석사례 등을 통해서 이해 할 수 있다.

셋째, 대화형 동적 분석(Interactive behavior analysis)방식이다.

자동화 분석 및 정적 분석이 이루어진다고 하더라도 실행코드에 대하여 모든 악의적인 행위를 정확하게 추적 할 수 없다. 레지스트리, 파일 시스템, 프로세스, 네트워크 활동을 이해하기 위해서 분리된 가상머신 환경에서 직접 테스트를 수행하면서 분석할 수 있다. 메모리 분석을 통해 다른 행위를 추가적으로 분석하는 부분도 고려할 수 있다. 대화형 동적분석은 악의적인 행위의 상세한 과정들을 확인할 수 있는 장점이 있지만, 분석가들의 분석 시간 소요가 많이 걸리기 때문에 반드시 필요한 분석인지를 선별하는 과정이 필요하다.

넷째, 수동 역공학 분석(Manual code reversing)방식이다.

코드를 역공학하여 분석하는 행위는 동적분석 과정안에 발생하는 분석 행위를 뜻할 수 있으며, 정적 분석이 완료된 후에 추가적인 정보를 획득하는데 분석하는 행위를 뜻한다. 아래와 같이 추가적인 분석과정의 예들이다.

- 특정 루틴에 난독화 되어서 복호화가 이루어지는 부분들이 있는지 추가적인 정보를 획득한다.
- 악의적인 도메인 생성과정의 알고리즘 분석
- 행동분석 과정에서 자신을 숨기고 보여주지 않았던 부분으로 발생되는 다른 기능 이해

따라서 소스코드까지의 정확한 검증은 소프트웨어의 규모나 코딩조건에 따라 상당한 비용과 시간면에서 불가능한 경우가 많을 수 있다. 그러나 일반적으로 P2P, 토런트, 커뮤니티사이트를 통해서 악성코드를 담고 있는 수많은 유틸리티들이 아무런 보안 검증도 없이 너무 많이 유통되고 있는 실정이다.

이러한 단순기능을 가지는 수많은 유틸리티는 오히려 점검하기가 쉽기 때문에 프로그램이 상용화 되지 않았다고 해서 점검을 소홀히 한다는 것은 일반 이용자들의 사이버위협과 사이버범죄어 노출되는 결과를 초래할 수 있다.

5. 안전한 소프트웨어 등록 시스템 구축 및 활용 방안

첫째, 소프트웨어 개발시에 안전성을 검증할 수 있는 정부나 민간기구 등이 필요하다.

현재는 P2P 및 인터넷 포탈, 커뮤니티 등의 웹 사이트에서 기본적인 소프트웨어에 대한 악성코드포함 여부를 확인한다고 하지만, 체계적이고 세부적으로 수행하지 않는다. 정부에서 승인하고 체계적으로 관리할 수 있는 기관이나 민간기구에서 검증업무를 부여할 필요성이 있다.

둘째, 어느 누구든 크고 작은 소프트웨어를 개발할 경우에는 보안성을 검증 받기위해 소프트웨어 안전성 평가 자율 등급제 도입이 필요하다.

이는 당장은 의무사항으로 하기에는 어렵다. 이러한 절차를 마련한다고 해도 수많은 개발 주체들이 소프트웨어 검증사이트에 등록하지 않을 거라는 추측이 가능하다. 단지 개발한 주체가 보안성이 검증된 안전한 소프트웨어라는 신뢰성을 받고자 한다면 'S/W 안전성 평가 체계'를 활용한 자율등급을 부여하여 유통하는 구조로 발전되어야 할 것이다.

셋째, 소프트웨어 대한 보안 안전성 인증 마크를 부여한다.

등록이 접수된 소프트웨어에 대해서는 소스코드 검증 및 악성코드 포함 여부를 확인하여 안전하다고 입증된 제품은 인증마크를 부여하고 등록을 유지시킨다.

넷째, 소프트웨어에 대한 본래의 해시값을 저장하고, 공유한다.

무분별한 소프트웨어 사용을 방지하기 위해서 인증된 제품에 대하여 다운로드가 가능하도록 하고, 제품을 구성하는 각각의 파일에 대하여 위·변조되지 않은 본래의 해시값을 저장하고, 해시값을 비교 검증할 수 있는 기능을 구축하여 사용한다.

(그림 8) 소프트웨어 등록 및 검증 절차

6. 결 론

현재에 국내에서는 공개소프트웨어나 불법 상용소프트웨어를 다운로드 할 수 있는 사이트가 넘쳐난다. 그러나 이러한 사이트의 보안 안전성 검증 및 불법 소프트웨어를 단속하는 기능은 미비한 실정이다.

사이버공격은 취약한 소프트웨어에 악성코드를 숨겨놓거나, 신뢰되지 않은 파일 공유사이트에서 무분별하게 다운로드 되고 있다. 이를 대응하기 위해서 소프트웨어 보안 검증 체계를 마련하고 신뢰성 있는 정보공유사이트를 구축 활용하면 사이버보안 강화에 도움이 될 것이다.

물론 개발된 소프트웨어가 등록시스템에 검증되지 않았다고 해서 모두 보안이 취약한 소프트웨어로 취급할 수는 없다. 단지 사용자 입장에서 검증된 소프트웨어를 사용하기 위한 최소한의 선제적인 방지 차원에서 수용할 수 있는 방안을 추가적으로 연구하는 것도 가능할 것으로 판단된다.

참 고 문 헌

[1] 소프트웨어산업진흥법
[2] www.moneys.news
[3] http://www.nis.go.kr
[4] https://zeltser.com/mastering-4-stages-of-malware-analysis
[5] http://chogar.blog.me/80211426900
[6] 한국정보통신기술협회 TTA 저널
[7] 소프트웨어정책연구소 https://spri.kr/
[8] https://www.tmmi.org/
[9] 한국인터넷진흥원(소프트웨어 개발보안)
[10] 모바일 전자정부 서비스관리지침 (행정자치부 고시 제2014-1호, 2014.11.25)
[11] App Annie (2017. 1) "App Annie 2016 Retrospective"

◐ 저 자 소 개 ◑

여 동 균

1999년 3월~2007년 6월(해군 정보통신 대위 전역)
2010년 10월~2011년 12월(통신 ISAC)
2012년 1월~현재(이글루시큐리티 보안관제 팀장)
2015년~현재 한국정보보호심사원협회(KISCA) 부회장
2016년~현재 한국사이버감시단 이사
관심분야 : 정보보호, 보안관제, IoT, 빅데이타, ISMS(Information Security Management System)
공동특허 : 인증 전원 제어시스템(제 10-1672926호.2016.10.31)

공 병 철

1999년~현재 (사)한국사이버감시단 대표이사
2002년~현재 (사)한국인터넷정보학회 부회장
2015년~현재 한국정보보호심사원협회 회장
2015년~현재 (주)에스링크(S-LINK) 대표이사
관심분야 : 정보보호, 지능정보사회, 클라우드 컴퓨팅 보안, IoT보안, 빅데이타보안,
ISMS(Information Security Management System)

이 근 혁

1986년 9월~2001년 12월(ISP사 및 KERIS 연구원)
2002년 1월~2004년 1월 한국통신사업자연합회 (정보통신부)통신ISAC 대외정보팀장
2004년 2월~2006년 6월 한국인터넷진흥원 (정보통신부)통신ISAC 부장
2006년 7월~2012년 12월 (방송통신위원회)통신정보공유분석협회(ISAC) 사무국장
2013년 3월~현재 한국정보통신진흥협회 (미래창조과학부)정보통신ISAC 부장
관심분야 : 정보보호, 취약점진단, IoT보안, 빅데이타보안, ISMS(Information Security Management System)