



Software 안정성을 위한 정적분석 연구

A study on Static Analysis for Software Safety

저자 (Authors)	홍재신, 박두순 Jae-sin Hong, Doo-Soon Park
출처 (Source)	한국멀티미디어학회 학술발표논문집 , 2007.11, 158-158 (1 pages)
발행처 (Publisher)	한국멀티미디어학회 Korea Multimedia Society
URL	http://www.dbpia.co.kr/Article/NODE01619167
APA Style	홍재신, 박두순 (2007). Software 안정성을 위한 정적분석 연구. 한국멀티미디어학회 학술발표논문집, 158-158.
이용정보 (Accessed)	순천향대학교 220.69.208.143 2016/03/15 13:30 (KST)

저작권 안내

DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다.

이 자료를 원저작자와의 협의 없이 무단게재 할 경우, 저작권법 및 관련법령에 따라 민, 형사상의 책임을 질 수 있습니다.

Copyright Information

The copyright of all works provided by DBpia belongs to the original author(s). Nurimedia is not responsible for contents of each work. Nor does it guarantee the contents.

You might take civil and criminal liabilities according to copyright and other relevant laws if you publish the contents without consultation with the original author(s).

Software 안정성을 위한 정적분석 연구

홍재신, 박두순
순천향대학교 컴퓨터학과
e-mail : zzuri@sch.ac.kr

A study on Static Analysis for Software Safety

Jae-sin Hong*, Doo-Soon Park**

*Dept. of Computer Science, Soonchunhyang Univ.

**Division of Computer Science and Engineering, Soonchunhyang Univ.

요 약

우리는 소프트웨어들의 보안에 대한 아무런 보장도 없이 사용해가고 있다. 소프트웨어 장애로 인한 악영향을 막기 위해 소프트웨어 보안이 요구되고 있지만 점점 소프트웨어의 크기가 대형화, 복잡화 되면서 이러한 일은 더욱 어려워지고 있다. 대용량 소프트웨어의 취약성에 대한 정보는 공격의 요소인 동시에 방어 기법을 개발하는 근간을 제공하는 가장 중요한 요소이다. 따라서 본 발표에서는 이러한 취약성들을 감소하기 위한 방법으로 정적 분석 방법들에 대한 동향을 조사하고 분석한다. 또한 기존에 제시된 도구 중 CIL(C Intermediate Language)과 CodeScroll™ Inspector Ver 1.0을 이용하여 공개 소스 코드들과 상용 도구에 대해서도 테스트한다. 이러한 결과를 토대로 대용량 소프트웨어 안전성 및 품질 향상을 위한 정적 분석 방법을 제안하고, 그에 따른 안전성과 효율성 그리고 취약성 검사 방법들에 대해서 분석한다.

1. 서론

지식 정보화 사회는 자연과 자본이라는 전통적인 생산 요소보다 지식이 중심 생산 요소로 부각되는 사회이다. 얼마나 많은 지식과 정보를 보유하고 있는냐에 따라 국가와 기업 또는 개인의 경쟁력이 결정되게 된다. 우리는 이러한 지식과 정보를 얻기 위해서 컴퓨터 소프트웨어를 사용하게 되고, 이러한 소프트웨어들의 보안에 대한 보장도 없이 소프트웨어에 의존해 살아가고 있다. 소프트웨어 보안에 대한 무지는 은행 시스템과 같은 장애로 이미 우리에게 심대한 피해를 준바 있다.

본 논문에서는, 이러한 소프트웨어 보안 취약성에 대해서 알아보고 실제 보급되고 있는 상용 분석

툴들을 적용·분석하여 보안 취약성 패턴들을 분류하고 검사하기 위한 소프트웨어 정적 분석 기술 방법을 제안한다.

2. 소프트웨어 취약성 분석

본 장에서는 소프트웨어 보안 취약성 중 버퍼 오버플로우(Buffer Overflow), 포맷 스트링 버그(Format String Bug)에 대한 취약성 분석을 기술한다.

2.1 버퍼 오버플로우 취약성 분석

버퍼 오버플로우는 데이터 저장을 위해서 설정