

# 시큐어 코딩 가이드의 기준과 문제점의 대안

유승민

고려대학교 컴퓨터정보통신 대학원  
소프트웨어 보안 학과  
e-mail : ryusm@korea.ac.kr

## Applying Secure Coding Standard And Alternatives to problems

Seung-Min Ryu,  
Software Security,  
Korea University Graduate School of Computer & Information technology

### 요 약

한국 소프트웨어 시장에 맞는 시큐어 코딩 가이드 기준을 설립하고, 이를 통하여 경제적인 비용을 절감 시키는 등 소프트웨어 개발을 효율적이고 안전성을 갖게 하는 것을 목표로 한다.

### 1. 서론

먼저 용어 정의에 대해 이야기 해보려 한다. OWASP에서는 Secure Coding 이란 CLASP 란 컨셉으로 순수한 Coding 에서의 보안이 아닌 개발 단계에 따른 보안 컨셉을 적용 시키는 것을 목표로 한다.[1]

소프트웨어 시장에서 흔히 하는 말로 “버그 없는 프로그램은 없다” 라는 것처럼 완벽한 보안은 불가능 하다.

기술 개발의 속도는 보안 기술의 발전보다 훨씬 빠르기 때문에(표 1) 이에 따른 보안 기술 발전의 속도가 더욱 더 중요해질 것으로 예상 한다.

그러나 최선의 보안을 보장하는 프로그램 개발을 위해서는 정의, 개발, 유지보수 단계 모든 단계에서 보안을 고려하는 방법이 필요하다.(그림 1)



(그림 1) 개발 방법론의 각 단계[3]

### 2. 현재 국내에서의 Secure Coding Standard 상황

국내에서의 Secure Coding Guide 는 KISA(한국인터넷진흥원) 에서 나온 SW 개발 보안 가이드를 통해 확인해 볼 수 있다.[3]

그러나 이런 기준은 개정 이후에 다른 이슈가 바로 발생 하더라도 바로 반영하기 어려운 것이 현실이다. 이런 부분 때문에, 보안 취약점 이슈를 따라가지 못하고 있는 것이 현실이다.

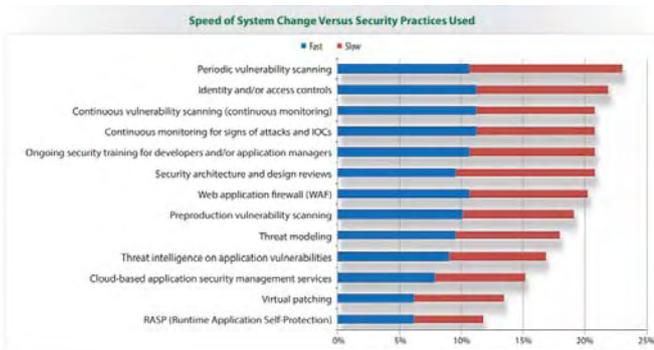
그 예로 JAVA 의 Secure Coding Guide 는 2012년 9월 이후 업데이트 되지 않고 있다. 또한 C 의 Secure Coding Guide 는 2012년 9월 3판 이후로 개정되지 않았다.

이런 문제 점을 보완하기 위해서 정부적 차원에서 보안 문제점의 중요성을 인식하고 이를 개선하려는 노력이 필요해 보인다.

### 3. 결론

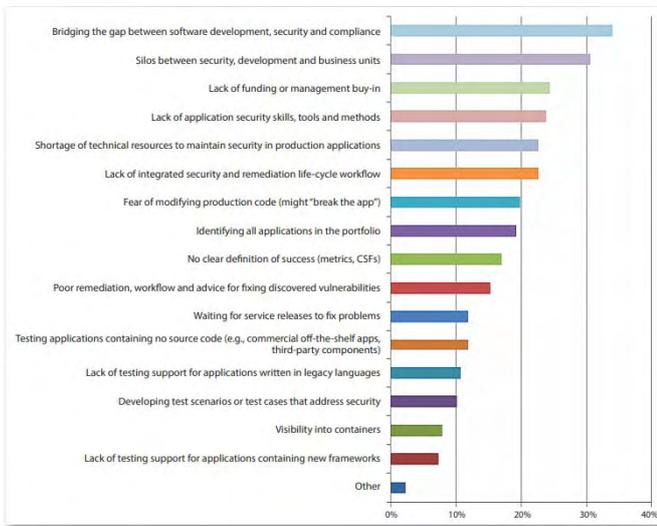
(표 2) 에서 확인 가능 하듯이 보안 구현 시 가장 큰 3 가지 당면과 과제 중 첫 번째로 “소프트웨어 개발, 보안 및 규정 사이의 격차 해소를 꼽았다.

구체적으로는 각 단계별 시큐어 코딩 가이드는 존재 하나 이를 지속적으로 업데이트 하고 규정의 디테일을 제시해 준다면, 결론적으로 정부 차원의 소프트웨어 개발과 보안 및 규정이 존재하고 이를 소프트웨어



(표 1) Speed of System Change Verse Security Practices Used[2]

어 개발 단계에 녹아낼 수 있다면, 개발론적인 관점에서 보안적인 관점에서도 두 마리 토끼를 모두 잡아 낼 수 있을 것이다.



(표 2) What are your three challenges in implementing application security for production systems at your organization? [2]

### 참고문헌

- [1] OWASP CLASP Concepts : [https://www.owasp.org/index.php/CLASP\\_Concepts](https://www.owasp.org/index.php/CLASP_Concepts)
- [2] 2017 State of Application Security : Balancing Speed and Risk : <https://www.sans.org/reading-room/whitepapers/application/2017-state-application-security-balancing-speed-risk-38100>
- [3] KISA : SW 개발보안가이드 <https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=259&dno=88&fseq=1>
- [4] KISA : JAVA Secure Coding Guide : [https://www.kisa.or.kr/public/laws/laws3\\_View.jsp?cPage=6&mode=view&p\\_No=259&b\\_No=259&d\\_No=55&ST=T&SV=](https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=55&ST=T&SV=)