무기체계 내장형 소프트웨어 시큐어 코딩 프레임워크

최문정*, 최준성**, 정익래*
*고려대학교 정보보호대학원
**삼성탈레스(주)
e-mail : cybersecurekr@gmail.com

Secure coding framework for the weapon systems embeded SW

Moonjeong Choi*, Junesung Choi**, Ikrae Jeong*
*Korea University CIST
**SAMSUNG THALES

요 약

사이버전의 위협은 종전에는 정보체계와 인터넷망에 국한되는 것으로 여겨졌으나 현재에는 망분리 환경이나 정보체계가 아닌 소프트웨어에 대해서도 위협이 실제하고 있으며, 그 공격 양상이 다양화 복합화 되는 경향을 보이고 있다. 향후 사이버전은 융복합 무기체계가 포함하고 있는 다양한 내장형 소프트웨어에 공격으로 확대될 것이며, 이에 따라 무기체계 내장형 소프트웨어에 대한 사이버전 대응 준비가 필요하다. 본 논문에서는 무기체계 내장형 소프트웨어의 사이버전 대응을 위한 방안으로 무기체계 내장형 소프트웨어의 보안성 강화를 위한 보안강화코딩(시큐어 코딩)을 적용 보안 프레임워크를 제안한다.

1. 서론

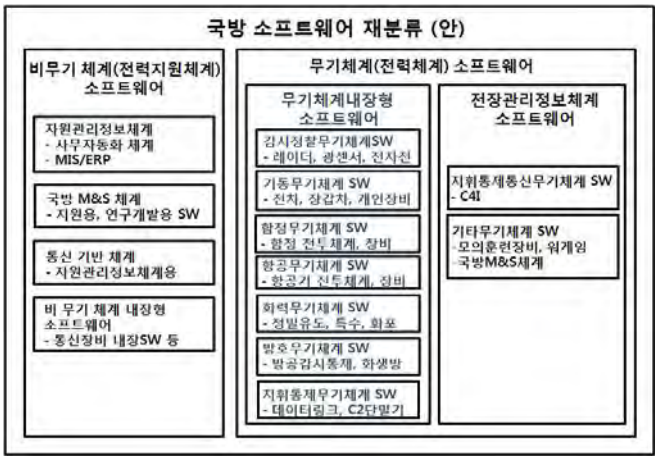
사이버전 위협은 다양화 복합화 되는 경향을 보이고 있다. 또한 망분리가 된 정보체계에 대해서도 사이버 위협들이 실제하고 있음이 입증되고 있다[1][2]. 향후 사이버전의 양상은 지휘통제용 정보체계에 대한 마비를 위한 사이버 공격 뿐만 아니라 융복합 무기체계의 다양한 기능 소프트웨어에 대한 마비를 위한 사이버 공격까지 확대될 것이다[1][2]. 남한은 사회기반과 군의 지휘통제체계에서 북한에 비해 정보화 의존도가 높기 때문에, 사이버전 발생 시 북한에 비해 물리적, 심리적 타격이 클 것으로 예상되는데, 무기체계의 기능 수행 자체에 대한 사이버 공격이 발생하는 경우에는 더욱 큰 타격이 발생될 것을 예상할 수 있다. 그러므로 무기체계 소프트웨어에 대한 사이버전 대응 준비가 필요하며, 본 논문에서는 무기체계 내장형 소프트웨어의 사이버전 대응을 위한 방안으로 무기체계 내장형 소프트웨어의 보안성 강화를 위해 보안강화코딩(시큐어 코딩)을 적용하는 보안 프레임워크를 제안하고자 한다.

2. 관련 연구

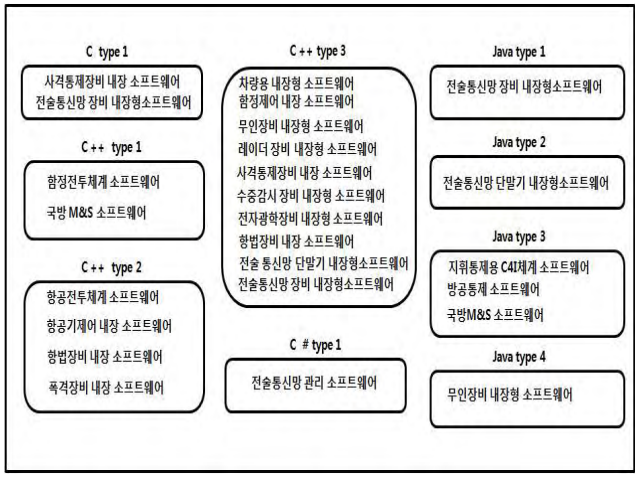
무기체계 내장형 소프트웨어에 시큐어 코딩을 적용하여 개발보안을 향상시키는 방안에 대해서는 무기체계별 시큐어 코딩룰의 최적 선정 방안을 중심으로 연구가 진행되어 오고 있다[1~11]. 이러한 연구들은 기존의 소프트웨어 개발보안과 시큐어 코딩이 전자정부 웹서비스와 안드로이드 웹서비스에 한정된 접근이었던 것에 비해, 무기체계내장형 소프트웨어에 대한 개발보안 적용을 고려한 점과 무기체계별 내장형 소프트웨어가 가진 특성을 고려하여 개별 무기체계 내장형 소프트웨어와 개발언어들을 기능과 특성별로 집단화하고 이 특성에 따라 무기체계 특성에 따라 기능별, 개발언어별 최적화된 시큐어 코딩룰을 선정하려고 했다는데 의미가 있다[1~11]. (그림1)의 국방 소프트웨어 재분류에서는 기존의 무기체계 분류보다 상세한 분류를 제시하고 있다[1][2][5][8].

(그림2)의 기능별, 개발언어별 시큐어 코딩룰 분류에서는 현재 활용되고 있는 개발 언어를 기준으로 무기체계 내장형 소프트웨어의 기능별, 개발언어별 특성을 고려하여 시큐어 코딩룰 타입이 필요함을 제시하고 있다[1][5]. 해당 분류는 현행 무기체계 SW

와 향후 개발 예정 SW에 대한 소요를 분석한 것이다[1][5].



(그림 1) 무기체계 기준 무기체계 소프트웨어 분류



(그림 2) 기능별/개발언어별 시큐어 코딩룰 분류

기존 연구에서는 무기체계 내장형 소프트웨어에 대한 시큐어 코딩 적용을 위한 코딩룰 자체의 선정을 중심으로 연구가 이루어지고 있어, 개발보안 적용을 위한 방법론에 대해서는 논의되지 못하고 있는 한계가 있다. 이에 본 논문에서는 시큐어 코딩 적용을 위한 보안 프레임워크를 중심으로 논하고자 한다.

3. 무기체계 내장형 소프트웨어에 대한 시큐어 코딩 프레임워크

무기체계 내장형 시큐어 코딩 프레임워크는 무기체계 내장형 소프트웨어의 생명주기를 고려하여 무기체계 내장형 소프트웨어에 대한 개발 계획, 개발, 개발보안 적용, 유지보수, 통제 및 감독을 수행하는 형태로 구성하고자 한다. 이러한 형태는 한국 정부에서 채택한 범정부 EA 프레임워크를 근간으로 하는 것으로 적용이 용이할 것으로 판단된다.

범정부 EA 프레임워크는 프레임워크 분야에서 사실 표준은 Zackman 프레임워크를 활용하여 구성된 것[12]으로, 본 논문에서 제안하고자 하는 무기체계 내장형 시큐어 코딩 프레임워크 역시 사실 표준인 Zackman 프레임워크를 활용하는 것으로 하고 있다.

무기체계 내장형 시큐어 코딩 프레임워크는 무기체계 내장형 소프트웨어의 생명주기를 고려하여 생애주기 영역을 가진다. 생애주기 영역에서는 계획 관점, 설계 관점, 개발 관점, 운영 관점의 네 가지 요소의 적용을 고려한다. 무기체계 내장형 시큐어 코딩 프레임워크는 개발과 유지보수를 고려하여 기능요소 영역을 가진다. 기능요소 영역에서는 목적기능 관점, 기술적용 관점, 보안 관점, 방호 관점의 네 가지 요소의 적용을 고려한다. 무기체계 내장형 시큐어 코딩 프레임워크는 통제 및 감독 수행을 고려하여 범위 선정 영역을 가진다. 범위 선정 영역에서는 정책의 적용으로 소프트웨어 개발보안과 관련된 정부의 정책을 적용을 고려한다. 다음으로, 소프트웨어 개발보안 적용을 위한 표준의 적용 즉, 선정된 시큐어 코딩룰의 활용을 고려한다. 마지막으로, 적용조직 관점으로 소프트웨어 개발보안의 적용조직과 검증 및 진단 조직(정적/동적 테스트 및 침투테스트 조직)을 고려한다.

4. 결론

본 논문에서는 무기체계 내장형 소프트웨어의 사이버전 대응을 위한 방안으로 무기체계 내장형 소프트웨어의 보안성 강화를 위해 보안강화코딩(시큐어 코딩)을 적용하는 보안 프레임워크를 제안하였다.

무기체계 내장형 소프트웨어 개발보안은 그 필요성에 비해 연구자가 한정되어 있어, 많은 관심과 발전이 필요한 분야이다. 향후에는 기존에 연구되던 무기체계별 특성에 따른 시큐어 코딩룰 선정 중 연구되지 않은 분야에 대한지속 연구와 기존에 선정된 코딩룰들에 대한 정교화가 필요하며, 침투테스팅과 연계한 실질적인 개발보안 방안 등에 대해서도 연구가 필요할 것이다.

참고문헌

[1] Junesung Choi, Development of Evaluation Model for Secure Coding Rule Selection Optimized on the System Characteristics, Seoul National University of Science and Technology

[2] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, Defense SW Secure Coding Application Method for Cyberwarfare Focused on the warfare System Embedded SW Application Level, Journal of Korea Association of Defense Industry Studies, 2012, Vol.19, No. 2, pp91-103.

[3] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, Evaluation Method Using Analytic Hierarchy Process for C4I SW Secure Coding Rule Selection, The Journal of Korea Information and Communication Society, 2013, Vol.38. No.8, pp 651-661.

[4] Junesung Choi, Kwangho Kook. Secure Coding Rule Selection Optimized on the Army Fire Control Computer, Journal of Security Engineering, 2014, Vol.11.No2, pp187-194.

[5] Junesung Choi, Kwangho Kook, Developing Warfare System SW Development Security Classification System Using KJ method, Journal of Security Engineering, 2014, Vol.11.No2, pp 165-176

[6] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, Naval Combat Management System Secure Coding Rule Selection Using Warfare System SW Secure Coding Rule Selection Evaluation Model, Journal of Security Engineering, 2013, Vol.10. No.4, pp417-428.

[7] Junesung Choi, Moonjeong Choi, Wonhyung Park, Kwangho Kook, Secure Coding Rule Selection for NCW Infrastructurem, KACE Proceeding, 2013.

[8] Junesung Choi, Wooje Kim, Kwangho Kook, Warfare System Embedded SW Secure Coding Application Method, 2012 KORMS Proceedings, pp1454-1466, 2012

[9] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho Kook, Developing Method for Secure Coding Rule for Command & Control Warfare System Embeded Software, Information Science / Information Processing Society Joint Symposium, 2013

[10] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho, Analysis on Secure Coding Rule Optimization Case for Warfare System Software Specificity, 2013 KORMS Proceedings, 2013

[11] Junesung Choi, Wooje Kim, Wonhyung Park, Kwangho, Selection Method for Software Security Development Characteristics Using Kano and QFD, KACE Proceeding, 2014

[12] HK Yang, HJ Cha, YG Choi, Study on the reform of a defence IT governance system, Jornal of KICS vol35. no5. pp 777-784, 2010