P R O J E C T D O C U M E N T

문제점 개요서

Project Name	Fuzz Testing을 통한 위성 SW 분석

05 조

202002473 김승혁
201902733 이정윤
202002699 조민기

지도교수: 이성호 교수님 (서명)

Document Revision History

Rev#	Date	Affected Section	Author
1	2025/03/18	초고 작성	김승혁
2	2025/03/19	2. 내용 수정	이정윤

Table of Contents

List of Figure

그림 목차 항목을 찾을 수 없습니다.

1.Survey Paper - Limitations Focus

번호	연구 제목(저자)	저널/컨퍼런스 (연도)	주요 내용 요약	한계점
1	Scaling Software Security Analysis to Satellites: Automated Fuzz Testing and Its Unique Challenges	USENIX Security Symposium (2024)	위성 소프트웨어의 보안 취약점을 분석하는 데 자동화된 퍼징(Fuzz Testing) 기법을 도입하는 방법을 연구한다. 기존 수작업 방식의 보안 분석이 확장성이 떨어지는 문제를 해결하기 위해 퍼징을 적용하고, 실제 위성(ESTCube-1, OPS-Sat, Flying Laptop)에서 발생할 수 있는 문제들을 분석한다.	특정 위성 시스템(ESTCube-1, OPS-Sat 등)에 초점을 맞추어 연구 결과의 범용성이 부족했다. 또한, 연구의 목적이 보안 분석에 국한되어 있어, 일반적인 소프트웨어 결함(버그) 탐색에는 충분히 활용되지 않았다.
2	Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software for Agile Mission Development	IEEE ACCESS (2021)	CubeSat과 같은 나노위성의 비행 소프트웨어에 퍼징 기법을 적용하여 결함을 자동으로 발견하는 방법을 연구한다. 테스트는 University of Chile의 SUCHAI-II, SUCHAI-III, PlantSat 위성 소프트웨어에 적용되었으며, 기존 테스트 방식보다 빠르게 12개의 결함을 발견하고 수정할 수 있음을 보여준다.	연구가 CubeSat의 특정 비행 소프트웨어(SUCHAI)에 한정되어 있어 연구 결과의 범용성이 부족했다. 또한, Fuzz Testing 과정에서 Code Coverage에 대한 분석 및 개선에 대한 내용이 부족했다.
3	Analysis of Vulnerabilities in Satellite Software Bus Network Architecture	IEEE Military Communications Conference (2022)	NASA 의 오픈소스 위성 운영 소프트웨어인 core Flight System(cFS)의 보안 취약점을 분석한다. 특히, 소프트웨어 버스(SB)를 이용한 통신 구조에서 인증이 부족하여 공격자가 쉽게 명령을 실행할 수 있다는 점을 강조하며, 네 가지 주요 공격 사례를 시연하고 이에 대한 보안 강화 방안을 제안한다.	cFS 기반 오픈소스 위성 소프트웨어의 취약점을 분석했지만, 연구 범위가 보안 이슈에 국한되어 있으며, Fuzz Testing 과 같은 자동화된 결함 탐색 기법을 활용하지 않았다. 또한, 특정 시스템(cFS) 및 통신 구조에 초점을 맞추었기 때문에 다른 위성 소프트웨어에도 적용 가능한 범용적인 분석이 부족하다.

2.Limitations and Research Gaps

번호	기존 연구	한계점	연구 필요성	본 연구의 기여
1	Scaling Software Security Analysis to Satellites: Automated Fuzz Testing and Its Unique Challenges	특정 위성 시스템(ESTCube-1, OPS-Sat 등)에 초점을 맞추어 연구 결과의 범용성이 부족했다. 또한, 연구의 목적이 보안 분석에 국한되어 있어, 일반적인 소프트웨어 결함(버그) 탐색에는 충분히 활용되지 않았다.	특정 위성 시스템이 아닌, 오픈소스 소프트웨어에 대한 연구가 필요하며, 보안 분석이 아닌 일반적인 소프트웨어 결함(버그)를 효과적으로 찾기 위한 연구가 필요하다.	본 연구는 특정 오픈소스 위성 소프트웨어를 선정하여 퍼징을 수행하고, 보안 취약점뿐만 아니라 일반적인 소프트웨어 버그를 자동으로 탐색함으로써, 퍼징 기법이 오픈소스 위성 소프트웨어 개발 과정에서 결함 탐지에 효과적임을 보인다.
2	Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software for Agile Mission Development	연구가 CubeSat의 특정 비행 소프트웨어(SUCHAI)에 한정되어 있어 연구 결과의 범용성이 부족했다. 또한, Fuzz Testing 과정에서 Code Coverage에 대한 분석 및 개선에 대한 내용이 부족했다.	특정 위성 시스템이 아닌, 오픈소스 소프트웨어에 대한 연구가 필요하며, Fuzz Testing에서 Code Coverage를 중점으로 성능을 개선한 연구가 필요하다.	본 연구는 특정 오픈소스 위성 소프트웨어를 선정하여 퍼징을 수행하고, Code Coverage 개선을 중점으로 연구하여, 기존 보다 더 넓은 범위에서 버그를 효율적으로 찾아낼 수 있음을 보인다.
3	Analysis of Vulnerabilities in Satellite Software Bus Network Architecture	cFS 기반 오픈소스 위성 소프트웨어의 취약점을 분석했지만, 연구 범위가 보안 이슈에 국한되어 있으며, Fuzz Testing과 같은 자동화된 결함 탐색 기법을 활용하지 않았다. 또한, 통신 구조에 초점을 맞추었기 때문에 다른 위성 소프트웨어에도 적용 가능한 범용적인 분석이 부족하다.	통신 구조 및 보안 분석이 아닌 위성 소프트웨어의 전반적인 영역에서 효과적으로 결함을 찾기 위한 연구가 필요하다.	본 연구는 보안 및 통신 구조에 국한되지 않고, Fuzz Testing을 통한 자동화 탐색으로 전반적인 영역에서 효율적으로 소프트웨어 버그를 찾아낼 수 있음을 보인다.