##### Project Document

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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Survey Paper – Limitations Focus 5](#_Toc192581443)

[2. Limitations and Research Gaps 6](#_Toc192581444)

List of Figure

그림 목차 항목을 찾을 수 없습니다.

# 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. | 퍼징을 위성 소프트웨어 보안 분석에 적용하는 가능성을 탐색했지만, 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. | CubeSat의 특정 비행 소프트웨어(SUCHAI)에서 퍼징을 수행했지만, 특정 시스템에 한정되어 있어 연구 결과의 범용성이 부족했다. 또한, 주어진 환경에서 발견된 일부 버그를 분석하는 데 그쳤으며, 퍼징을 통해 탐색 가능한 다양한 유형의 결함에 대한 체계적인 분석이 부족했다. |
| 3 | The Integration and Testing Procedures for the  AcubeSAT Nanosatellite’s Software | 20th International Conference on Synthesis  (2024) | AcubeSAT 미션의 소프트웨어 통합 및 테스트 절차를 설명하며, 특히 맞춤형 하드웨어 환경에서의 안정성을 확보하기 위한 다양한 검증 기법을 소개한다. 위성의 온보드 컴퓨터, 자세 제어 시스템, 통신 모듈 등과 같은 핵심 시스템을 통합하여 ESA의 PUS-C 표준을 준수하는 방식으로 개발 및 테스트를 진행했다. | 이 연구는 위성 소프트웨어의 통합 및 테스트 절차를 다루었지만, 특정 미션(AcubeSAT)에 초점을 맞추고 있어 범용성이 부족하며, 퍼징을 활용한 자동화된 결함 탐색 기법이 포함되지 않았다. 또한, 연구가 주로 시스템 통합 및 테스트 절차에 집중되어 있어, 개별 소프트웨어의 결함을 탐색하는 데에는 한계가 있다. |
| 4 | Analysis of Vulnerabilities in Satellite Software Bus  Network Architecture | MILCOM  (2022) | NASA의 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 위성 소프트웨어의 보안 취약점을 분석했지만, 연구 범위가 보안 이슈에 국한되어 있으며, 퍼징과 같은 자동화된 결함 탐색 기법을 활용하지 않았다. 또한, 특정 시스템(cFS)에 초점을 맞추었기 때문에 다른 위성 소프트웨어에도 적용 가능한 범용적인 분석이 부족하다. |

# 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 | 기존 연구는 퍼징을 위성 소프트웨어 보안 분석에 적용하는 가능성을 탐색했지만, 특정 위성 시스템(ESTCube-1, OPS-Sat 등)에 초점을 맞추어 연구 결과의 범용성이 부족했다. | 연구의 목적이 보안 분석에 국한되어 있어, 일반적인 소프트웨어 결함(버그) 탐색에는 충분히 활용되지 않았다. | 본 연구가 어떻게 기존 연구의 한계를 해결하는지 구체적으로 설명  연구 기여를 정량적/정성적으로 설명 (예: 성능 개선, 새로운 접근법 제안 등)  본 연구는 특정 오픈소스 위성 소프트웨어를 선정하여 퍼징을 수행하고, 보안 취약점뿐만 아니라 일반적인 소프트웨어 버그를 자동으로 탐색함으로써, 퍼징 기법이 위성 소프트웨어 품질 향상에 어떻게 기여할 수 있는지를 연구한다. |
| 2 | Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software | 기존 연구는 CubeSat의 특정 비행 소프트웨어(SUCHAI)에서 퍼징을 수행했지만, 특정 시스템에 한정되어 있어 연구 결과의 범용성이 부족했다. |  | 본 연구는 특정 오픈소스 위성 소프트웨어를 선정하여 퍼징을 수행하고, Fuzz Testing을 통해 다양한 유형의 버그를 발견하여 보다 일반화된 연구 결과를 제공할 것이다. |
| 3 | The Integration and Testing Procedures for the  AcubeSAT Nanosatellite’s Software | 기존 연구는 주로 시스템 통합 및 테스트 절차에 집중되어 있어, 개별 소프트웨어의 결함을 탐색하는 데에는 한계가 있다. | 특정 미션(AcubeSAT)에 초점을 맞추고 있어 범용성이 부족하며, Fuzz Testing을 활용한 자동화된 결함 탐색 기법이 포함되지 않았다. | 본 연구는 특정 오픈소스 위성 소프트웨어를 선정하여 Fuzz Testing을 수행하고, 자동화된 방식으로 다양한 버그를 찾아내어 위성 소프트웨어의 신뢰성을 높이는 데 기여할 것이다. |
| 4 | Analysis of Vulnerabilities in Satellite Software Bus  Network Architecture | 기존 연구는 연구의 범위가 보안 이슈에 국한되어 있다. | Fuzz Testing과 같은 자동화된 결함 탐색 기법을 활용하지 않았다. | 본 연구는 특정 오픈소스 위성 소프트웨어를 선택하여 퍼징을 수행함으로써, 보안뿐만 아니라 일반적인 소프트웨어 결함을 탐색하고 위성 소프트웨어의 안정성을 높이는 데 기여할 것이다. |