드론 펌웨어 역공학 방지를 위한 난독화 연구

연동현[1], 장대희[2]
[1]경희대학교 컴퓨터공학과 학부생
[2]경희대학교 컴퓨터공학과 교수
ydh1214@khu.ac.kr, daehee87@khu.ac.kr

Anti-Reverse Engineering of Drone Firmware through Obfuscation Technique

Dong-Hyeon Yeon[1], Dae-Hee Jang[2]
[1]Dept. of Computer Engineering, Kyung-Hee University
[2]Dept. of Computer Engineering, Kyung-Hee University

요 약

드론 산업의 급속한 성장과 함께, 드론 펌웨어에 대한 보안이 중요한 이슈로 대두되고 있다. 본 연구는 드론 펌웨어를 보호하기 위한 효과적인 방법 중 하나로 소프트웨어 난독화 기술을 제안한다. 난독화 기법은 소스 코드나 바이너리를 의도적으로 복잡하게 변형시켜, 외부의 불법적인 분석 및 변조를 어렵게 만드는 방법이다. 이 연구는 드론 펌웨어에 대해 난독화 기법을 적용하고, 그 효과를 평가함으로써 드론 시스템의 보안 강화에 기여하고자 한다.

1. 서론

최근 몇 년간 드론 기술은 빠르게 발전해왔다. 이러한 발전은 다양한 산업 분야에서 혁신적인 적용 가능성을 제시하며, 우리의 삶과 사회에 새로운 가능성을 열어주고 있다. 드론은 초기에는 주로 군사 및 항공 사진 촬영에 사용되었지만, 현재에는 농업, 배송, 인프라 관리, 구조 작업 및 엔터테인먼트 등 다양한 분야에서 활용되고 있다[1]. 이러한 드론 기술의 발전과 함께 보안 도전 과제도 중요해지고 있다. 특히, 드론 펌웨어에 대한 무단 접근 및 변경은 개인의 사생활 침해, 비인가된 영역에서의 비행, 심지어는 테러리즘에 이용될 가능성을 내포하고 있다. 이러한 보안 과제는 드론 기술의 발전을 뒷받침하며, 본 연구에서는 드론 펌웨어에 대한 역공학 방지를 목적으로 소프트웨어 난독화 기술의 적용 가능성을 탐구한다.

2. 난독화 기술과 드론 펌웨어 보안

2.1 드론 펌웨어 보안 동향

최근 드론 보안 기술은 주로 두 가지 주요 분야에서 발전을 거듭하고 있다. 첫 번째 영역은 통신 링크의 암호화 및 인증 메커니즘의 강화하는 것이고, 두 번째는 펌웨어 자체의 보안 강화에 주목하고 있다. 특히, 드론 펌웨어에 대한 무단 접근을 차단하기 위한 보안 기술의 개발이 점점 더 중요해지고 있으며, 이를 위한 안티 리버싱(Anti-reversing) 기법의 중요성이 부각되고 있다. 현존하는 보안 기술만으로는 역공학의 완전한 방지가 어렵기 때문에, 펌웨어의 안티 리버싱 기법의 개발이 절실히 요구된다[2]. 이러한 맥락에서, 난독화 기법은 프로그램의 이해와 분석을 복잡화함으로써 역공학 과정을 시간 소모적이고 어렵게 변화시키는 유효한 접근법으로 제시되고 있다[3].

2.2 소프트웨어 난독화 기법의 분류와 원리

소프트웨어 난독화는 소스 코드나 실행 파일을 복잡하게 만들어 역공학을 어렵게 하는 기술이다[4]. 이는 소프트웨어 보안 강화에 핵심적인 역할을 하며, 구조적 난독화, 데이터 난독화, 알고리즘 난독화 등으로 분류된다. 구조적 난독화는 가짜 코드 삽입과 불필요한 분기를 통해 실행 흐름을 복잡하게 만들고, 데이터 난독화는 변수 이름 변경과 데이터 구조 재구성을 통해 분석을 방해한다. 알고리즘 난독화는 소프트웨어 내부의 알고리즘 또는 계산 과정을 복잡하게 만드는 기법이다.

3. 펌웨어 난독화 기법 적용

3.1 드론 펌웨어 난독화 적용 예시

본 연구는 드론의 이륙 프로세스에 난독화 기법

적용을 목표하였다. 이를 위해, OLLVM(Obfuscator LLVM)이라는 오픈소스 난독화 도구를 활용하여 펌웨어에 난독화를 시도하였으나, PX4-FMUv6x 펌웨어를 실제로 난독화 처리할 시, 빌드 환경의 컴파일러 버전과 PX4 시스템 라이브러리 간 호환성의 문제가 드러났다. 이에, 본 연구에서는 <표 1>에 기술된 바와 같이, 난독화 과정을 수동으로 조정하고 TakeoffHandling::updateRamp 모듈에 더미 코드 8줄을 추가하여 프로세스를 빌드하였다.

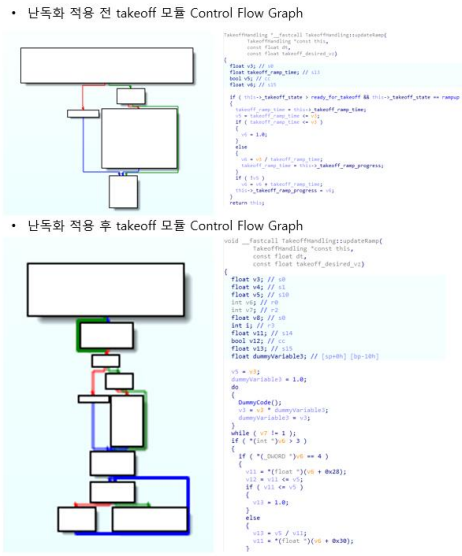
```
1  int dummyCounter = 5;
2  for (int i = 0; i < dummyCounter; ++i) {
3    if (i % 2 == 0) {
4      //미미한 변경 후 즉시 변경 취소
5      upwards_velocity_limit += 0.0001f;
6      upwards_velocity_limit -= 0.0001f;
7    }
8  }
```

<표 1> 이륙 프로세스 난독화: 더미 코드 적용 예시

3.2 난독화 구현 및 빌드 방법

본 연구의 구현 단계에서는, 드론 펌웨어의 보안을 강화하기 위한 난독화 기법 중 더미 코드 삽입과 제어 흐름 변조를 중점적으로 적용하였다. 이 방법은 코드의 직관성을 저하시키고, 역공학 과정을 복잡하게 만들어 분석을 어렵게 한다. 난독화 적용 과정에서는 빌드 최적화 레벨을 조정하여, 난독화된 코드가 컴파일러에 의해 제거되지 않도록 하였다.

드론 펌웨어 난독화 기법의 적용은 (그림 1)과 같



(그림 1) IDA에서 확인한 난독화 전후 이륙 프로세스 흐름 비교(하늘색 부분은 프로세스 초기에 선언되는 변수)

이 이륙 프로세스 CFG(Control Flow Graph)의 변화 등으로 코드 분석이 더 어려워진 것을 확인할 수 있었으며, 이는 난독화가 역공학 방지에 유효한 수단임을 시사한다. 이후 본 연구에서 수정된 펌웨어 바이너리를 드론 시스템에 플래싱하여 실제 비행 테스트를 수행하였고, 테스트 결과 문제없이 비행할 수 있음을 확인할 수 있었다.

4. 결론 및 향후 연구 방향

본 연구는 드론 펌웨어의 보안 강화에 난독화 기법을 적용하는 방안을 탐구하였다. 난독화 기법의 적용은 드론 펌웨어의 복잡성을 증가시켜, 무단 접근자에 의한 이해와 분석을 어렵게 만드는 효과적인 방법임이 입증되었다. 난독화 기법이 드론 보안에 기여할 수 있는 잠재력을 확인함으로써, 드론 시스템의 무단 역공학 및 코드 분석으로부터의 보호라는 중요한 목표 달성에 대한 기초를 마련하였다. 이는 드론 기술의 안전성과 신뢰성 향상에 중요한 첫걸음을 의미한다. 하지만 동시에, 펌웨어의 빌드 과정과 난독화 도구 간의 호환성 문제와 같은 기술적 도전 과제도 드러났다. 이는 난독화 기법의 실제 적용을 위한 중요한 고려 사항으로, 향후 연구 및 개발 과정에서 해결해야 할 주요 과제이다.

사사표기

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 융합보안핵심인재양성사업의 연구 결과로 수행되었음" (IITP-2024-RS-2023-00266615*)

참고문헌

[1] 항공안전기술원, 국내외 드론 산업 현황 조사 https://www.droneportal.or.kr/subList/20000000028

[2] Gaurav Kumar, "A Survey on Program Code Obfuscation Technique," Engineering and Technology Journal, vol. 1, no. 2, 2016.

[3] B. Cyr, J. Mahmod and U. Guin, "Low-Cost and Secure Firmware Obfuscation Method for Protecting Electronic Systems From Cloning," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3700-3711, April 2019.

[4] Nagra, Jasvir, and Christian Collberg. Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection: Obfuscation, Watermarking, and Tamperproofing for Software rotection. Pearson Education, 2009.