2023 전기 졸업과제 착수보고서

USB 키보드 펌웨어 변조 연구

36. 키보드 워리어

분과 : D

학번	201724546
이름	이창율
학번	202055607
이름	차현수
학번	201924619
이름	당낫투안

목차

1. 과제 배경 및 목표

1-1. 과제 배경

최근 많은 키보드가 매크로, 키 바인딩, RGB 조명 등의 기능을 지원하기 위해 펌웨어를 탑재하고 있다. 또한 펌웨어의 버그 수정 및 기능 개선을 위해 업데이트 기능도 제공하고 있다. 키보드 펌웨어를 통해 컴퓨터로 전달되는 데이터는 사용자의 입력 정보를 다루기 때문에 민감한 정보를 포함할 가능성이 높지만, 키보드 펌웨어 변조에 대한 연구는 부족하다.

1-2. 목표

- 키보드 펌웨어의 변조 가능성을 분석하고, 이를 활용한 공격 시나리오 도출.
- 변조된 키보드 펌웨어를 통해 쉽게 제거할 수 없는 악성 행위 구현.
- 안전하지 않은 키보드 펌웨어 업데이트 과정의 취약함에 대한 인식을 제고.
- 키보드 펌웨어의 보안 강화를 위한 대응 방안 도출.

2. 연구 과정

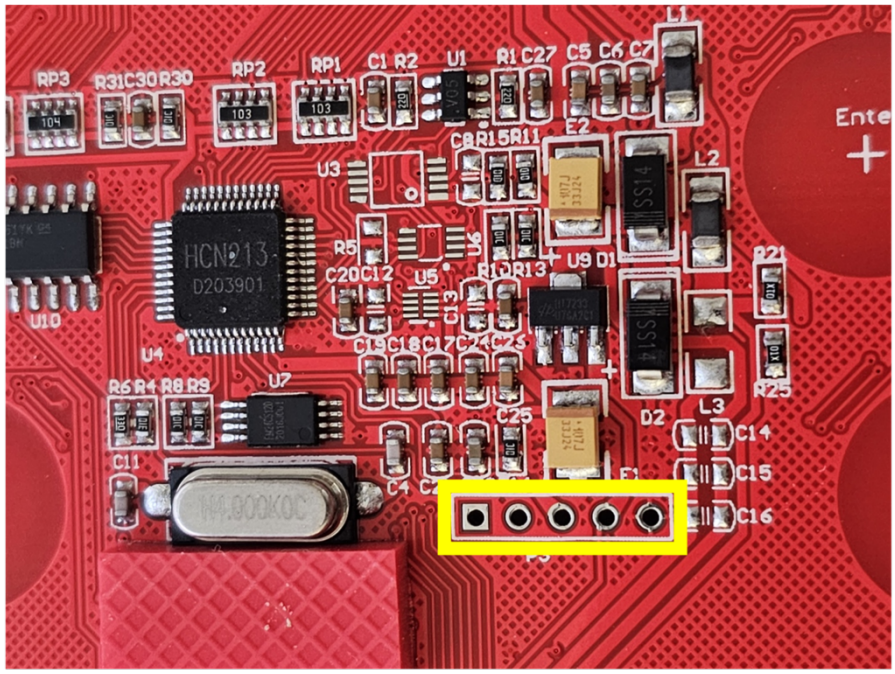
2-1. 키보드 펌웨어 획득 및 분석

2-1-1. 펌웨어 획득

키보드 펌웨어를 분석하기 위해 먼저 펌웨어를 구해야 한다. 펌웨어를 얻는 방법으로는 크게 두 가지가 있는데, 하나는 키보드 제조사 홈페이지에서 다운받는 방법이고, 다른 하나는 ICSP(In-Circuit Serial Programming) 방식을 이용해 직접 키보드 칩에 포트를 연결하여 펌웨어를 추출하는 방법이다.

펌웨어를 구하는 첫 번째 방법을 이용해서 펌웨어를 얻어내면 펌웨어에 암호화가 되어 있는 경우가 있다. 이러면 해당 제조사의 펌웨어 업데이트 프로그램을 분석하여 복호화하는 방법을 알아낼 수 있다.

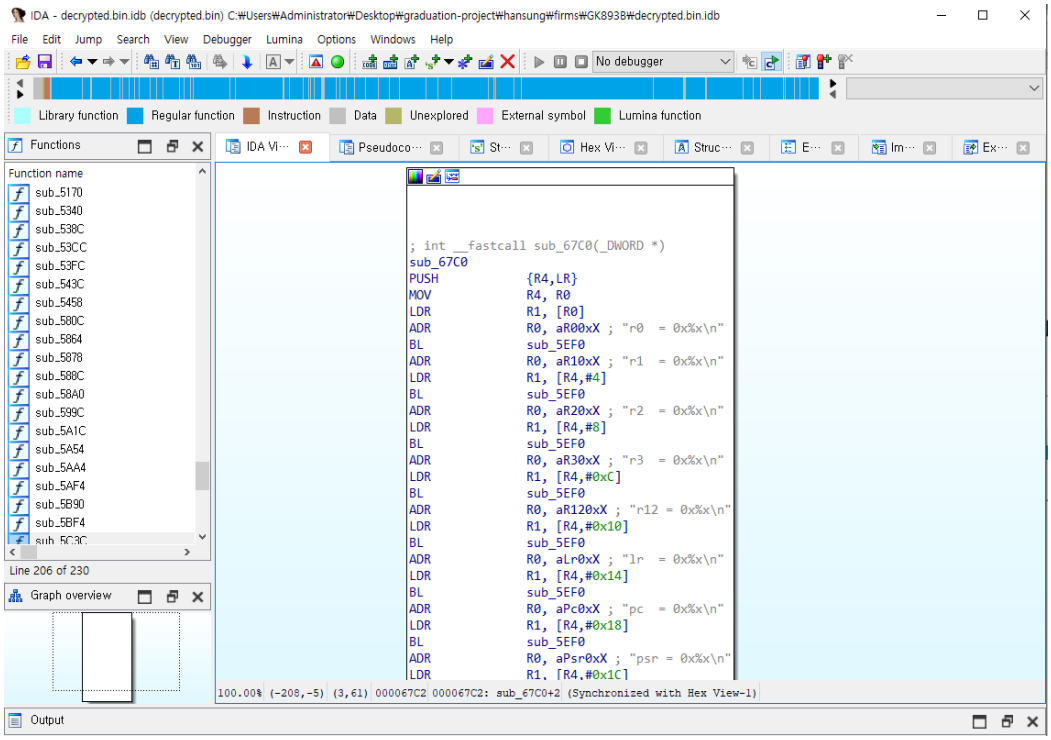
만약, 복호화에 실패하여 첫 번째 방법으로 펌웨어를 얻어내는 데 실패하면, 앞서 언급한 두 번째 방법으로 펌웨어를 얻어낼 수 있다.



〈 그림 1. ICSP 방식을 위한 Debug Interface 〉

2-1-2. 펌웨어 분석

앞서 설명한 방법으로 펌웨어를 획득하고 나면, 펌웨어를 조작하기 위해 분석해야 한다. 키보드 제조사에서 제공하는 데이터시트를 참고하여 IDA 와 Ghidra 와 같은 소프트웨어 역공학 도구를 사용하여 분석할 수 있다.



〈 그림 2. IDA 를 이용한 펌웨어 분석 〉

2-2. 악성코드 구현 방법

펌웨어 분석이 끝나면 다음 두 가지 방법으로 악성코드를 삽입할 수 있다.

첫 번째는 펌웨어에서 사용하지 않는 메모리 영역을 사용하여 악성 행위를 하는 코드를 삽입하고, 펌웨어를 변조하여 악성코드가 삽입된 영역으로 실행흐름을 바꾸는 방법이다.

두 번째는 오픈 소스로 공개된 키보드 펌웨어를 대상 키보드에 맞게 수정하고, 악성 행위를 하는 코드를 추가하여 대상 키보드로 변조된 펌웨어를 올리는 방법이다.

앞서 설명된 두 가지 방법 중 첫 번째 방법을 통해 주로 구현할 예정이며, 상세한 악성코드의 동작과 행위는 연구가 진행되며 구체적으로 정해질 예정이다.

2-3. 공격 시나리오 도출

키보드 펌웨어를 공식 사이트가 아닌 경로로 다운로드하거나, 공격자가 키보드 사용자의 시스템에 침투하여 키보드의 펌웨어를 임의로 업데이트하는 경우 키보드에 변조된 펌웨어가 설치될 수 있다. 또한 사용자가 중고 키보드를 구매하는 상황에서도 이미 변조된 펌웨어가 설치된 키보드를 구매하게 될 가능성이 있다.

이번 연구에서 위와 같은 방법을 포함하여 악성코드가 삽입되어 변조된 펌웨어가 올라간 키보드를 사용자가 사용하게 되기까지의 상세한 공격 시나리오를 만들어 볼 예정이다.

2-4. 대응 방안 도출

이번 연구를 통해 펌웨어의 변조를 막거나 변조된 펌웨어를 사용하지 못하게 하는 등의 대응 방안을 도출해 볼 예정이다. 이는 연구를 더 진행하여야 구체적인 방안을 도출할 수 있을 것이다.

3. 연구 일정 및 역할 분담

3-1. 연구 일정

#	항목	시작	종료	기간 (주)	날짜
					5/15 6/1 6/15 7/1 7/15 8/1 8/15 9/1 9/15 9/30
1	기초 지식 공부 (USB Internal, ARM)	6 / 1	6 / 21	3	
2	펌웨어 업데이터 분석	6 / 14	8 / 9	8	
3	펌웨어 분석	6 / 14	8 / 23	10	
4	변조된 펌웨어를 키보드로 업데이트 할 수 있는지 검증	6 / 14	9 / 7	12	
5	변조된 키보드를 통한 공격 시나리오 도출	6 / 21	8 / 2	6	
6	도출된 공격 시나리오를 기반으로 악성코드 구현	7 / 1	9 / 9	10	
7	대응 방안 도출	7 / 1	8 / 26	8	
8	미흡한 부분 보완 및 마무리	9 / 1	9 / 30	4	

3-2. 역할 분담

이름	역할
이창율	키보드 펌웨어 분석 키보드 펌웨어 분석 도구 개발 변조된 펌웨어 제작
차현수	키보드 펌웨어 분석 키보드 펌웨어 업데이터 분석 및 개발 변조된 펌웨어 제작
당낫투안	키보드 펌웨어 분석 펌웨어 변조 관련 논문 조사 및 자료 수집 키보드 펌웨어 분석을 위한 실험 환경 구성
공통	기초 지식 공부 보고서 작성 발표 및 시연 준비