36 USB 키보드 펌웨어 변조 연구

소속 정보컴퓨터공학부 분과 D 팀명 키보드워리어 참여학생 차현수, 이창율, 당낫투안 지도교수 권동현

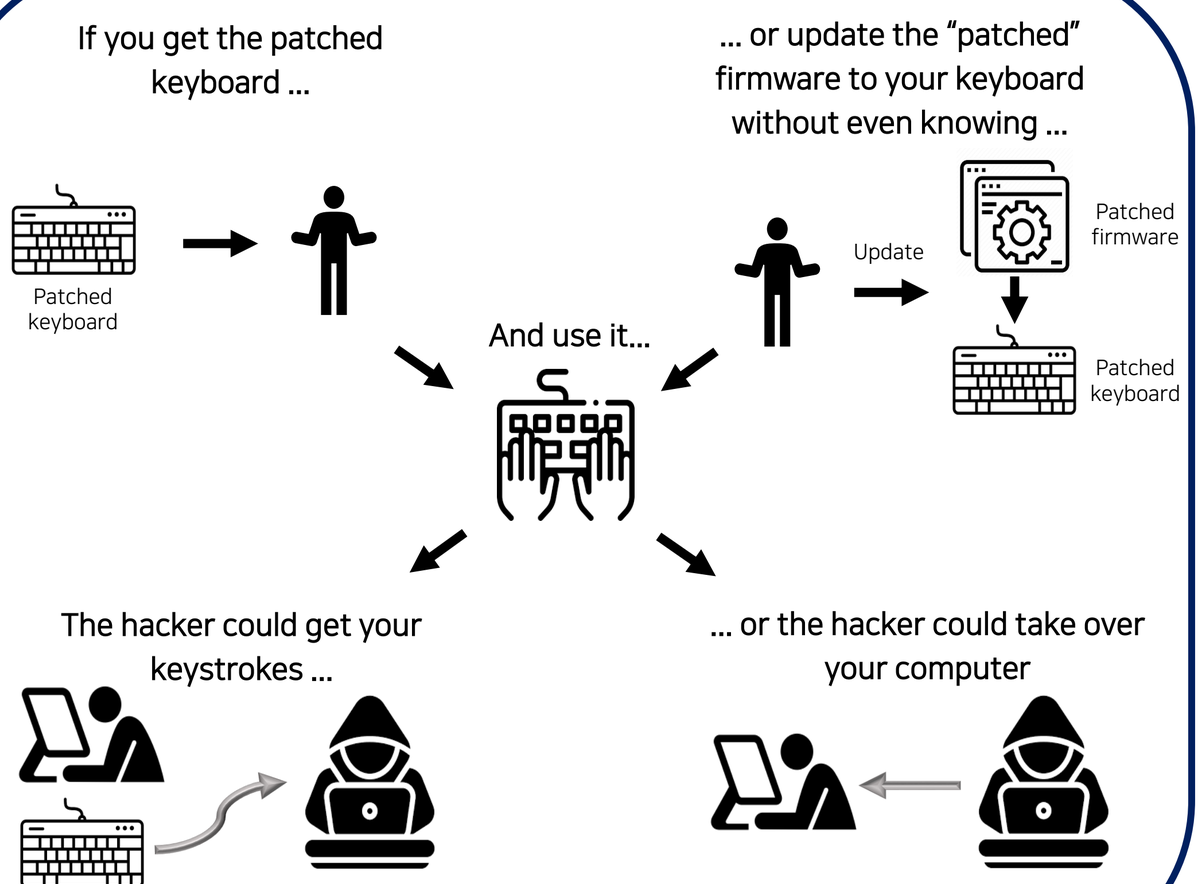
개요 및 목표

- ✓ 현대의 키보드는 **펌웨어**를 통해 텍스트 입력뿐만 아니라 다양한 기능들을 제공한다.
- ✓ 펌웨어는 사용자의 입력 정보를 다루기 때문에 **보안 측면에서 매우 중요**하다.
- ✓ 하지만, 키보드 펌웨어의 **보안에 관한 연구는 상대적으로 미흡**하다.

따라서, 키보드 펌웨어 변조 및 악성 행위 구현을 통해,
키보드 펌웨어 및 업데이트 과정의 취약함에 대한 인식을 제고한다.

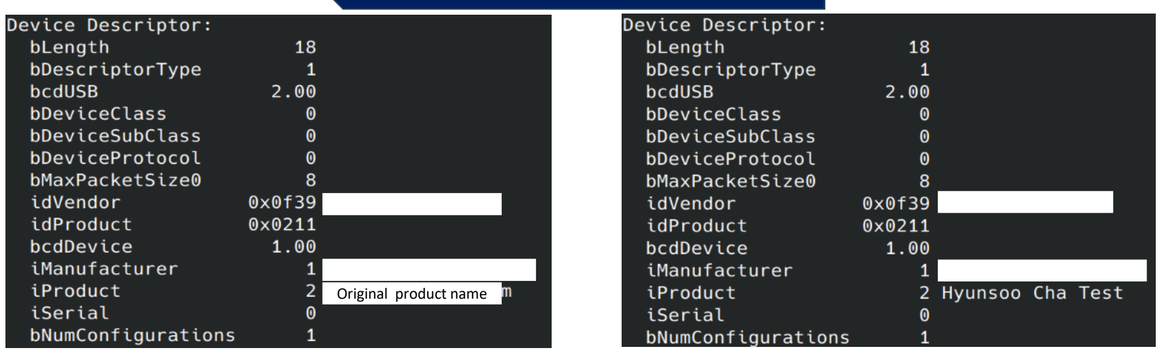
상세 내용

1. 공격 시나리오 구성



1. 연구 주제와 비슷한 논문 등을 참고하여 공격 시나리오를 구성했다.
2. 대상 키보드들의 펌웨어를 분석하고, 간단히 변조 가능성을 확인하였다.
3. 변조가 가능함이 확인되면, 펌웨어의 남는 저장 공간에 코드를 삽입하는 Code Cave 기법을 이용해 악성 행위를 구현하였다.

2. 펌웨어 변조 가능성 확인



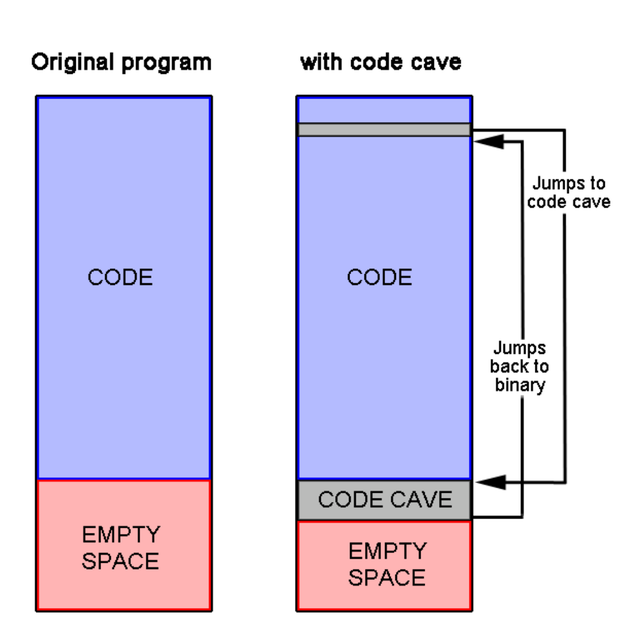
```
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            0
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0         8
  idVendor           0x0f39
  idProduct          0x0211
  bcdDevice            1.00
  iManufacturer           1
  iProduct                2  Original  product name
  iSerial                 0
  bNumConfigurations      1
```

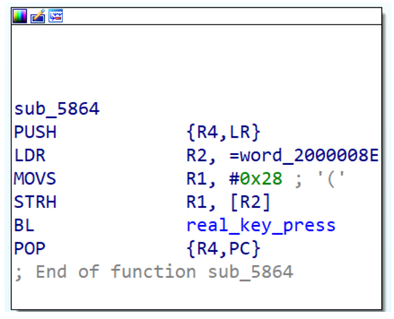
정상 펌웨어

```
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            0
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0         8
  idVendor           0x0f39
  idProduct          0x0211
  bcdDevice            1.00
  iManufacturer           1
  iProduct                2 Hyunsoo Cha Test
  iSerial                 0
  bNumConfigurations      1
```

변조된 펌웨어

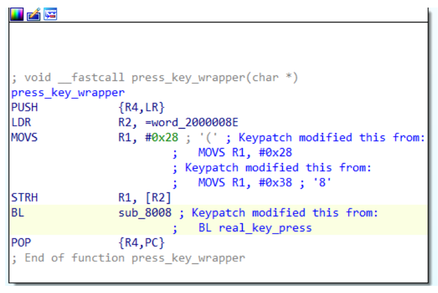
3. Code Cave 기법을 활용한 펌웨어 변조 및 악성 행위 구현





```
sub_5864
PUSH            {R4,LR}
LDR             R2, =word_2000008E
MOVS            R1, #0x28 ; '('
STRH            R1, [R2]
BL              real_key_press
POP             {R4,PC}
; End of function sub_5864
```

정상 펌웨어

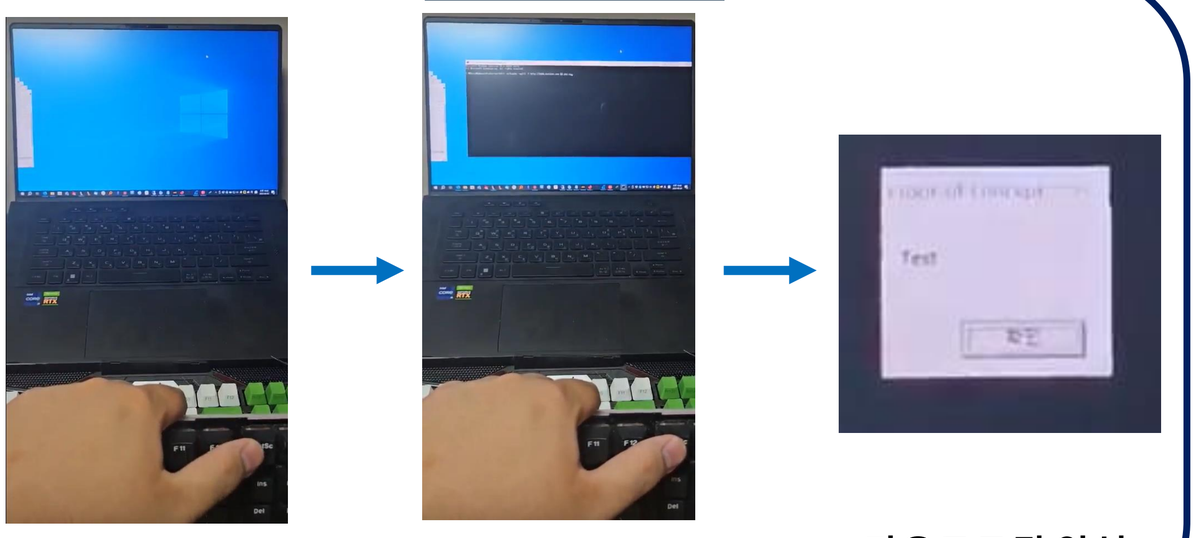


```
; void __fastcall press_key_wrapper(char *)
press_key_wrapper
PUSH            {R4,LR}
LDR             R2, =word_2000008E
MOVS            R1, #0x28 ; '(' ; Keypatch modified this from:
                          ;   MOVS R1, #0x28
                          ; Keypatch modified this from:
                          ;   MOVS R1, #0x38 ; '8'
STRH            R1, [R2]
BL              sub_8008 ; Keypatch modified this from:
                          ;   BL real_key_press
POP             {R4,PC}
; End of function press_key_wrapper
```

변조된 펌웨어

결과

구현 결과



펌웨어가 변조된 키보드 사용 → 악성 프로그램 다운로드 및 실행 스크립트 동작 → 다운로드된 악성 프로그램 실행

- ✓ 연구 대상 키보드 중 2개에 대해 악성 행위 구현에 성공했다.
- ✓ 일반적으로 사용하는 키보드의 펌웨어 업데이트 과정이 안전하지 않음을 보였다.
- ✓ 펌웨어 업데이트 과정에서 검증이 충분하지 않기 때문에 RSA 또는 ECDSA 같은 디지털 서명을 구현해 제조사에 의해 서명된 펌웨어만 업데이트하도록 해야 한다.