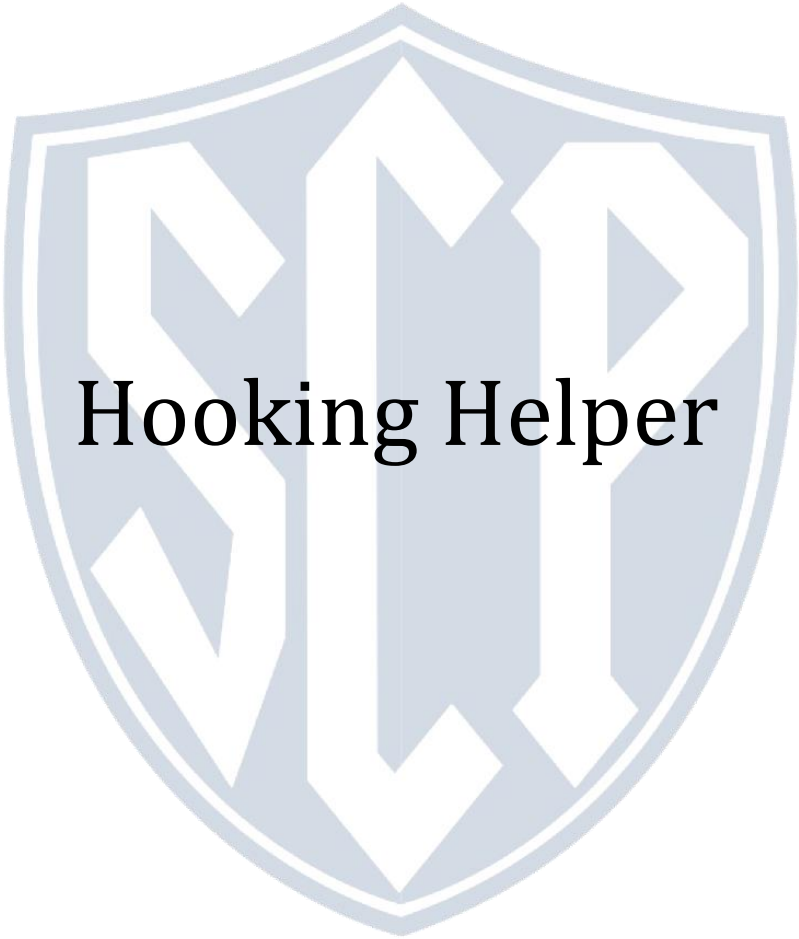
SCP 프로젝트 최종 보고서



Hooking Helper

프로젝트 참여자	팀장	송태현
	팀원	이유경

프로젝트 요약

- apk 파일이 주어지면 디컴파일 해주고 나온 폴더에서 mono방식일 경우 Assembly-Csharp.dll을 읽어주고, il2cpp 방식일 경우 dump시켜둔 dump.cs파일을 읽어서 원하는 오프셋을 찾습니다. 그 후 찾은 오프셋을 통해 후킹하여 값을 변조 시키는 스크립트를 짰습니다.

- apktool을 이용하여 apk 파일을 디컴파일 시켜주는 작업을 합니다.

- il2cppdumper을 이용하여 libil2cpp.so 파일을 dump 시켜 준 뒤 생성된 dump.cs 파일 속 함수의 offset을 가져와줍니다.

- frida를 이용하여 네이티앱을 후킹 시켜줍니다.

목차

1. 프로젝트 목표

- Unity로 구성된 게임을 후킹 하고 싶은데 자료가 안 나와서 못하는 사람들에게 unity게임을 후킹할 수 있게 도와줍니다.

- il2cppdumper와 apktool을 이용하여 apk파일을 디컴파일과 dump시키는 과정을 손쉽게 할 수 있게 도와주는 설명서 같은 프로그램을 제작하여 사람들을 도와줄 수 있는 프로그램을 만들려고 합니다.

- 다소 어렵고 자료가 많이 없는 후킹 스크립트를 자동으로 짜줘서 이용할 수 있게 도와주려고 합니다.

2. 프로젝트 수행

1. 현재 폴더에 apktool의 존재 여부를 확인 후, 없으면 다운 시켜줍니다.

```
def makedir(): #download or play
    path = "./"
    file_list = os.listdir(path)
    if "apktool_2.4.1.jar" in file_list:
        root = Tk()
        root.filename =  askopenfilename(initialdir = "./",title = "파일을 선택",filetypes = (("apk files","*.apk"),("all files","*.*")))
        apk_name = root.filename
        subprocess.call(['java','-jar',"./apktool_2.4.1.jar",'d','-f',apk_name])
    else:
        webbrowser.open("https://bitbucket.org/iBotPeaches/apktool/downloads/apktool_2.4.1.jar")
        a = int(input("다운을 한뒤 현재 스크립트가 실행되는 파일에 넣어주세요 다되셨으면 1을 입력 해주세요 ==>"))
        if a == 1:
            makedir()
```

2. 파일의 방식(mono/il2cpp)을 선택하는 과정을 진행합니다.

```
def choice_menu():
    choice = int(input("""
    이제는 mono 방식인지 il2cpp 방식인지 선택을 해야합니다.
    확인 방법은 hxd 를 열어서  apk 파일을 드래그 해서 올려 줍니다.
    그 뒤에 linmono , libil2cpp 파일이 있는지 확인을 해줍니다.
    libmono 파일이 있으면 1
    libil2cpp가 있다면 2
    hxd 가 없으시다면 3
    나가기는 4을 입력해주세요
    =>"""))
    if choice == 1:
        print("모노 방식입니다.")
    elif  2:
        print("il2cpp 방식은 한가지 과정이 더필요합니다.")
        a = int(input("il2cppdumper를 다운 한 적이 있으면 1번을 눌러주세요. 없으시다면 2번을 눌러 주세요"))
        if a == 1:
            b = int(input("il2cppdumper의 압축을 풀어서 현재 스크립트가 있는 곳으로 옮겨주세요. 되셨다면 1번을 눌러주세요."))
            if b == 1:
                il2cppdump_use()
        elif a == 2:
            webbrowser.open("https://github.com/Perfare/Il2CppDumper/releases/download/v5.1.0/Il2CppDumper-v5.1.0.zip")
            print("파일 다운로드가 끝났으면 압축을 푼뒤 현재 스크립트가 실행되고 있는 폴더에 넣어 주세요.")
            time.sleep(3)
            tcho = int(input("다 되셨으면 1을 눌러 주세요."))
            il2cppdump_use()
    elif 3:
        print("저런 다운로드 하셔야 겠네....가서 자신의 버전과 맞는것을 다운 받으세요.")
        webbrowser.open("https://mh-nexus.de/en/hxd/")
        choice_menu()
    elif 4:
        break
```

3. 쓰레딩을 통해 il2cppdumper를 실행 시킴과 동시에 gui환경으로 구성된 il2cppdumper 사용 설명서 띄웁니다.

```
def il2cppdump_use():
    a =int(input("1.나는 이 어플을 후킹하는 것이 처음입니다. \n2.il2cpp를 이용해서 이미 dump 시켰습니다."))
    if a == 1:
        os.chdir("./Il2CppDumper-v5.1.0")
        t = threading.Thread(target=lambda: os.system("Il2CppDumper.exe"), args=())
        t.start()
        il2cppdump_how()
        il2cppdump_use()
```

```
window=tkinter.Tk()
window.title("il2cppdumper 사용법!!")
window.geometry("640x400+100+100")
window.resizable(False, False)

notebook=tkinter.ttk.Notebook(window, width=600, height=400)
notebook.pack()

frame1=tkinter.Frame(window)
notebook.add(frame1, text="1.어플의 unity 버전 구하기")

label1=tkinter.Label(frame1, text='''먼저 아까 어플리케이션을 푼 폴더로 갑니다.
그 안에 /assets/bin/Data폴더에 들어가줍니다.
그 안에 있는 무작위 파일(폴더 아닙니다)을 hxd 에 넘겨 줍니다.
그 후 바로 보이는 (년도,월, 일)을 복사 해 둡니다.''')
label1.pack()

frame2=tkinter.Frame(window)
notebook.add(frame2, text="2.첫번째 파일 선택창에서 할 일")

label2=tkinter.Label(frame2, text='''Il2CppDumper를 실행 하겠습니다.
사용 방법은 그렇게 어렵지 않습니다.
창이 두개 뜰건데 처음 뜬 창에서는  먼저 우리가 아까 풀었던 파일을 들어 갑니다.
lib폴더에 있는 여러 방식중 자신이 구동하려는 버전의 폴더로 들어갑니다.
만약 자신이 에뮬레이터를 사용하면 x86,x64 를 들어 가시면 됩니다.
핸드폰인 경우 arm64 ,혹은 armeabi...인 파일에 들어가서 libil2cpp.so파일을 선택합니다.''')
label2.pack()

frame3=tkinter.Frame(window)
notebook.add(frame3, text="3.두번째 파일 선택창에서 할 일")

label3=tkinter.Label(frame3, text='''두번째에 뜬 창에서 선택해야 하는 파일은/assets/bin/Data/Managed/Metadata 안에있는 메타 데이터 파일입니다.
파일을 선택한뒤 무언가를 입력하라고 뜰텐데 그곳에 아까 복사한 (년도,월,일)을 입력해줍니다.
그 후 옵션을 선택하라고 나오는데 거기서 3을 누르면 dump 성공입니다.''')
label3.pack()

frame4=tkinter.Frame(window)
notebook.add(frame4, text="3.dump한뒤 해야 할 일")

label4=tkinter.Label(frame4, text='''il2cpp 폴더에 가셔서 Dummydll폴더와 dump.cs파일 script.py stringliter.json 파일을 한 폴더에 넣어 줍시다.
이 이후는 이 스크립트가 자동으로 함수의 오프셋을 찾아서 함수의 값을 변환 시켜 드릴 예정입니다.
메뉴에 없는 함수를 후킹 하실 계획 이시라면 직접 찾아서 해보시는 것을 추천 드립니다.''')
label4.pack()

window.mainloop()
```

4. 패키지 명을 구하는 과정을 진행합니다.

```
def il2cppdump_use():
    a =int(input("1.나는 이 어플을 후킹하는 것이 처음입니다. \n2.il2cpp를 이용해서 이미 dump 시켰습니다."))
    if a == 1:
        os.chdir("./Il2CppDumper-v5.1.0")
        t = threading.Thread(target=lambda: os.system("Il2CppDumper.exe"), args=())
        t.start()
        il2cppdump_how()
        il2cppdump_use()
    elif 2:
        OSF = []
        def packnam():
            a = input("apktool을 이용해서 생성된 폴더에 들어가서 경로를 복사해 붙혀주세요 ==> ")
            os.chdir(a)
            f_op = open("AndroidManifest.xml",'r')
            while True:
                line = f_op.readline()
                if not line:
                    break
                if "package" in line:
                    a=list(line.split(" "))
                    for b in a:
                        if "package" in b:
                            c=b.split('"')
                            k = c[1]
            f_op.close()
            return k
```

5. 원하는 함수의 오프셋을 구합니다.

```
ass = input("il2cppdumper를 이용해서 만든 dump.cs 파일이 있는 위치를 입력 해주세요. => ")
os.chdir("{}".format(ass))
ch_g = find_O()
f = open('dump.cs','r',encoding="utf-8")
if ch_g == 1:
    while True:
        line = f.readline()
        if not line: break
        if 'GetHPMaxBase' in line:
            a=list(line.split(" "))
            b=list()
            for i in a:
                if '0x' in i:
                    b.append(i)
            print("RVA값 ==",b[0],"offset값 ==",b[1])
            OSF.append(b[0])
```

6. 후킹 스크립트

```
cat = str(OSF[0])
dog = int(input("원하는 값 ===> "))
hook_code= """
function get_hook()
{{
    var il2cpp = Module.getBaseAddress("libil2cpp.so");
    var offset = {};
    var get_Attack = il2cpp.add(offset);

    Interceptor.attach(get_Attack,
    {{
        onEnter: function(args)
        {{
            console.log("^^b 후킹 성공");
        }},
        onLeave: function(retVal)
        {{
            var Attack = retVal.toInt32();
            var New_ATK ={};
            retVal.replace(New_ATK);
            console.log("change magic : "+Attack+" ->"+New_ATK);
            console.log("");
        }}
    }});
}}
Java.perform(function(){{
    get_hook();
}});
""".format(cat,dog)


device =frida.get_usb_device(timeout=10).attach(PACKAGE_NAME)
script = device.create_script(hook_code)
script.on("message",on_messege)
script.load()
sys.stdin.read()
```

3. 프로젝트 최종 결과

```
^^b 후킹 성공
change magic : 600 ->5000
```

4. 팀원 블로그

이유경	https://lyk00331.tistory.com/
송태현	https://r-ever-scp.tistory.com/