라즈베리 파이 4를 이용한 소형 자동화 해킹 툴 개발

한상훈*, 강병조O, 이영섭**, 이은수**
*한경국립대학교 컴퓨터응용수학부,
O한경국립대학교 평택캠퍼스 컴퓨터정보보안과,
**한경국립대학교 평택캠퍼스 컴퓨터정보보안과
e-mail: hansh0903@hknu.ac.kr*, kangcori@naver.comO, blacksea9697@gmail.com**, les1238@naver.com**

Handheld Automation Hacking Tool Development Using Raspberry Pi 4

Sang-Hoon Han*, Byeong-Jo KangO, Yeong-Seop Lee**, Eun-Soo Lee**
*School of Computer Engineering & Applied Mathematics, Hankyong National University,
ODept. of Computer Information Security, Hankyung National University Pyeongtaek Campus,
**Dept. of Computer Information Security, Hankyung National University Pyeongtaek Campus

● 요 약 ●

본 논문에서는 관련 지식이 없더라도 취약한 비밀번호를 사용하는 AP(Access Point)를 빠르고 편하게 점검할 수 있는 소형 해킹 장치를 제안한다. 터치 디스플레이를 이용한 입출력 장치의 통합으로 휴대성을 극대화시켰다. 필요한 정보를 특정하여 출력하고, 숫자 입력만으로 프로그램을 제어하며, AP의 보안 프로토콜 유형을 자동으로 인식하여 그에 맞는 공격을 시도하는 등의 사용자의 편의성을 고려한 프로그램 설계로 입력 장치의 제한으로 인해 생길 수 있는 불편함을 해소하였다.

키워드: 액세스 포인트(Access Point), 무선 네트워크 보안(Wireless Network Security), 해킹 툴(Hacking tool)

I. Introduction

정보화 사회에서 셀 수 없을 정도로 많은 정보가 무선 네트워크를 통해 전달된다. 하지만 대부분 사람은 편리한 사용에만 초점을 두고 취약한 보안에는 부족한 관심을 보인다. 최근에 꾸준히 발생하고 있는 IP 카메라 해킹사례를 보면 가정집은 물론, 대형 병원의 무선 네트워크의 보안대책도 너무나 취약하다는 걸 확인할 수 있었다[1].

이에 본 논문에서는 WPA2 무선 해킹 방법을 이용하여[2,3] 취약한 비밀번호를 사용하는 AP를 빠르고 편하게 점검할 수 있는 소형 해킹 장치를 제안한다.

II. The Proposed Scheme

라즈베리 파이와 같이 소형 컴퓨터를 이용한 해킹 툴 제작은 일반인들도 쉽게 시도할 수 있을 정도로 접근성이 좋다. 대부분의 제작 사례를 보면 소형 컴퓨터에 모니터와 키보드, 마우스 등의 입출력 장치를 연결하여 구성하는 경우가 많다. 이럴 때, 노트북과 같이 입출력 기기가 일체형으로 구성된 장치와 비교했을 때 오히려 휴대성과 편의성 측면에서 좋지 못하다. 따라서 소형 컴퓨터의 이점을 활용할 수 있도록 터치 디스플레이를 이용한 입출력 장치의 통합으로 휴대성을 극대화하고, 간단한 입력만으로 공격을 수행할 수 있도록 프로그램을 구성하였다.

1. Hardware Configuration

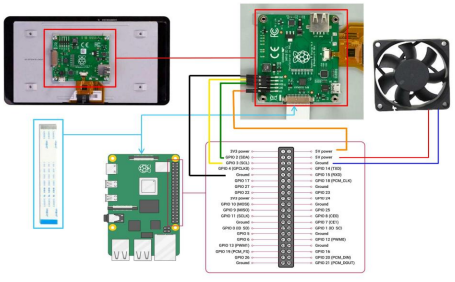

Fig. 1. Raspberry Pi 4 Circuit Diagram

그림 1은 라즈베리 파이 4, 쿨링팬, 터치 디스플레이를 연결하여 사용할 수 있도록 구성한 회로도이다. 인터페이스를 자유롭게 추가할 수 있으나, 본 논문에서는 휴대성을 위해 부피를 줄여 최소한의 인터페이스로 구성하였다.

2. Algorithm Flowchart

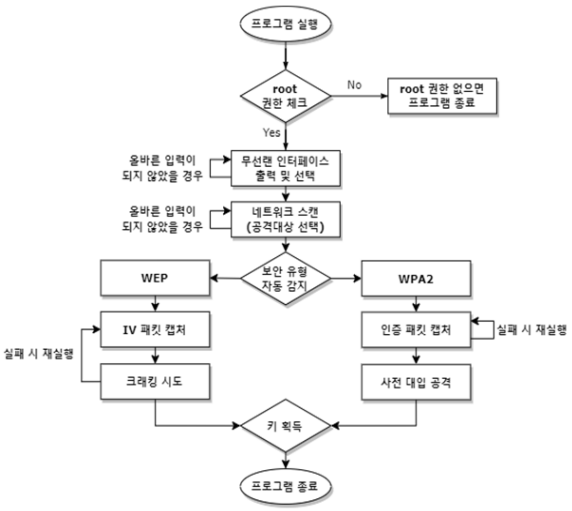

Fig. 2. Shell Script Flowchart

그림 2는 자동화를 위한 쉘 스크립트 구성 절차를 나타낸 것으로, 무선랜 인터페이스와 네트워크 선택 시 숫자 입력으로 선택이 가능하고, 공격 실패 시 자동으로 패킷을 추가 수집하기 때문에, 프로그램을 재실행하지 않고 공격 대상만 지정하면 결과가 나올 때까지 추가적인 입력 없이 AP에 대한 모니터링이 가능하다.

III. Experimental and Results

Fig. 3. Display of Program Execution

본 연구에서의 개발은 칼리 리눅스 상에서 Aircrack-ng 툴과 Bash shell script를 사용하였다. 그림 3과 같이 쉘 스크립트로 작성된 프로그램 실행했을 때, 정상적으로 작동하여 취약하게 설정된 AP의 크래킹이 가능했다. 휴대성을 높이고 소형화를 위해 터치 디스플레이를 사용하였으며, 입력의 제한 사항을 해결하기 위해 화상 키보드 기능을 이용하였다.

IV. Conclusions

본 논문에서 제안한 장치는 필요한 정보를 특정하여 출력하고, 숫자 입력만으로 프로그램을 제어하는 등의 사용 편의성을 고려하여 관련 지식이 없는 사람들도 쉽게 취약점 점검이 가능하도록 제작되었다. 라즈베리 파이의 확장성이 좋기 때문에 AP 취약점 점검뿐만 아니라, 다른 무선 장비의 취약점 점검 등의 추가 기능 개발이 가능하다. 이러한 점을 고려해서 향후 다른 점검 기능의 추가와 GUI 개발을 통해 사용자 편의성 상승 등을 고려하여 개발할 예정이다.

REFERENCES

[1] "Click' in the Living Room at Home and the Operating Room in the Hospital... Privacy Concerns Spread on Social Media, edaily, https://www.edaily.co.kr/news/read?newsId=01167686635737168&mediaCodeNo=257

[2] Jeo Soon, “A Study on Security Threat Detection Factor in a Wireless Environment”, Paichai University Graduate school, Master's degree thesis, 2014. 12.

[3] Han S.H., Koo K.R. Go E.S., Park H.S., Kim H.T., Song D.Y., “A Security Analysis by Cracking in Wireless Routers”, Procceedings of KSCI Conference 2017, Vol. 25, 2, pp 400-401.