제목 : 무선공유기 보안공격 분석 및 무료와이파이 해킹 해결방안

1. 연구 배경

- 공공 와이파이를 통한 네트워크 사용량이 증가함에 따라 무선공유기 해킹의 위험이 증가하고 있음.

- 무선공유기의 취약성으로 인해 해킹이 용이해지고 있어 대응책 필요성이 대두됨.

2. 주제

- 무료와이파이를 통한 보안공격과 해킹 대응방안 분석.

3. 핵심 내용 및 연구

- 와이파이에 사용되는 암호화 방식과 무선공유기의 보안 취약점을 분석.

  와이파이 암호화 방식 : WEP, WPA, WPA2

  *WEP (Wired Equivalent Privacy): RC4 암호를 사용하며, 40비트 키를 이용하여 데이터를 암호화,쉽게 해독될 수 있어 보안에 취약

  *WPA (Wi-Fi Protected Access): TKIP(Temporary Key Integrity Protocol)를 사용하여 WEP의 일부 요소를 재활용. WPA도 침투에 취약하며, WPS(Wi-Fi Protected Setup)를 통한 연결도 취약점으로 악용될 수 있음

  *WPA2: WPA2는 WEP와 WPA의 문제점을 개선한 버전으로, 가장 강력한 보안 기능을 제공

  무선 공유기 보안 취약점: ARP Spoofing, ICMP Redirect 공격

- 무료와이파이를 통한 해킹 사례를 조사하고 이를 해결할 수 있는 방안을 모색해야 한다고 주장

- 악의적인 스마트폰 접근과 악성 프로그램 설치로 인한 개인정보 유출 등의 보안 위협에 대해 체계적으로 대응해야 함.