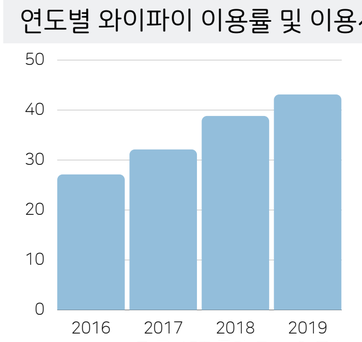
무선공유기 해킹으로 본 보안의 위험성

2020 과학기술대학 학술제
와이해킹 | 문지언 김다은 김지윤 이유진

문제 제기

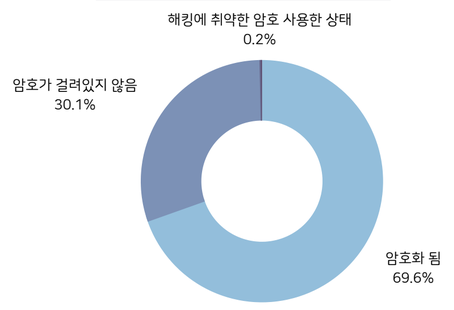
ICT 통계 정보 연구실의 2016년에서 2019년 사이 와이파이 이용률 조사 결과를 보면 이용률 수치가 꾸준히 증가하고 있음을 알 수 있다. 이용률 수치가 증가하는 것에 비해, 가정용 와이파이나 무료로 제공되는 공공 와이파이의 상당수는 암호화가 되어 있지 않아서 공격에 취약하다. 실제로 공유기를 해킹한 후 악성 앱을 유포하여 포털 계정을 부정 생성하는 등의 해킹 사례가 다분하다. 따라서 본 연구에선 직접 무선 공유기를 해킹하여 무선 공유기 보안의 위험성을 알아보고자 한다.

연도별 와이파이 이용률 및 이용시간



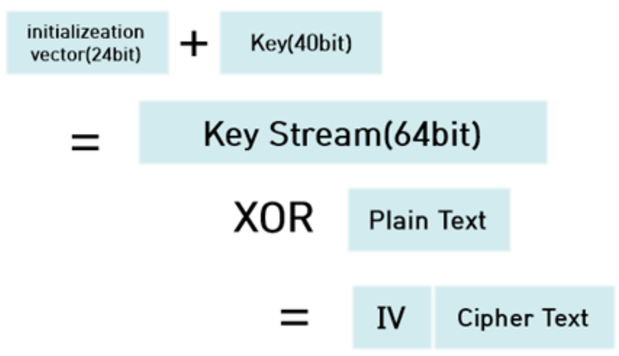
자료: ICT 통계 정보 연구실

와이파이 접속 상태 조사



WEP

- **WEP이란?**
  유선 랜에서 제공하는 것과 유사한 수준의 보안 및 기밀 보호를 무선 랜에서 제공하기 위하여 와이파이 표준에 정의되어 있는 보안 프로토콜
- **암호화 방식**



WEP 암호화 알고리즘으로는 스트림 암호화 기법인 RC4를 이용한다. 먼저, 24 bit의 IV(Initialization Vector) 값을 랜덤하게 생성하고 Key 값 40비트가 더해져 총 64비트 Key Stream 생성한다. 그 다음 평문과 Key Stream을 XOR 연산하여 생성된 암호문 앞에 IV값을 추가하여 전송한다.

WEP 취약점

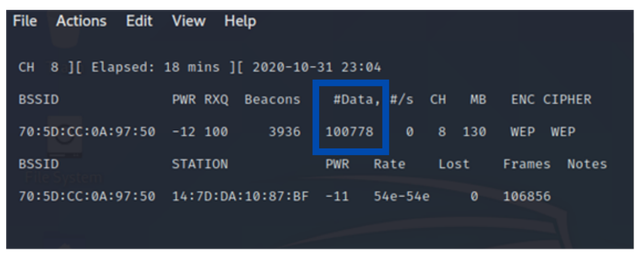
- IV 가 24비트로 너무 짧아서 IV값을 랜덤하게 생성하는 과정에서 짧은 길이로 인해 반복 사용될 경우가 있다.
- Key 값이 절대 변하지 않아서 IV + Key 값으로 이루어진 키 스트림에서의 Key 값은 불변이므로 많은 패킷을 수집해 Weakness IV를 통해 Key Stream을 모아 비교한다면 Key 값이 노출된다.

*Weakness IV : Key에 대한 정보를 노출시키는 IV값

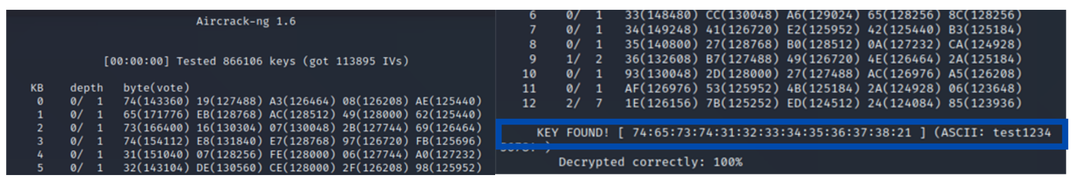
WEP 연구과정

IV는 총 24bit로 3byte로 이루어져 있다. IV값 중에서 키 스트림의 첫 번째 Byte에는Weakness IV값이 있다. 패킷을 암호화할 때 IV값은 계속 바뀌지만 Weakness IV값은 바뀌지 않고 그대로 사용되게 된다. 즉, Weakness IV값을 충분히 수집하여 WEP Key를 추측 할 수 있다. 따라서 많은 패킷을 모아야 crack확률이 올라간다.

1. Weakness IV값을 모으기 위해 패킷을 수집한다. 128 Bit WEP Key를 이용했기 때문에 약 1,500,000개의 IV값을 가진다. 따라서 Data를 100,000개 정도 모았다.

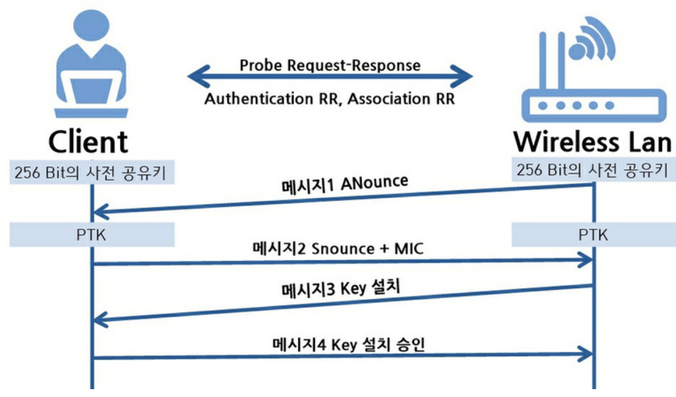


2. 수집된 패킷으로부터 Weakness IV값을 추출해 비밀키를 추측한다.



WPA

- **WPA이란?**
  원래의 Wi-Fi 보안 표준인 WEP보다 개량된 프로토콜
  WEP에 비해 보다 정교한 데이터 암호화를 제공, 사용자 인증이 다소 불충분했던 WEP와는 달리 완전한 사용자 인증 기능을 제공함
- **암호화 방식**



WPA1과 WPA2은 사전 공유키(PSK, Pre_Shared Key)와 다섯 개의 매개변수(network SSID, ANounce, SNounce, AMAC Address, SMAC Adress)를 이용해서 일대일 대칭 키(PTK, Pairwise Transient Key)라는 Session Key를 계산한다. Client와 Wireless Lan은 PTK를 사용하여 모든 데이터를 암호화한다.

WPA 취약점

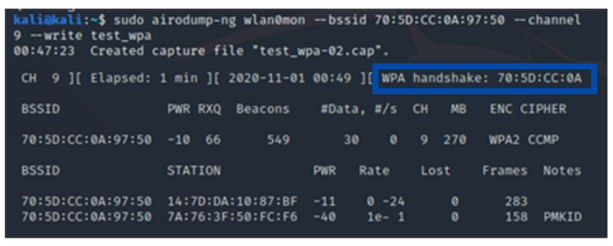
- 클라이언트와 무선랜과의 인증 절차를 노려서 해킹할 수 있다.
- 인증 절차에서 4 Way Hand Shaking 과정을 거치는데, 인증 패킷 스니핑을 통해 PSK와 변수 5개 (network ssid, ANounce, SNounce, AMAC Address, SMAC Address)가 적힌 패킷을 캡쳐하여서 암호를 알아낼 수 있다.

*4 Way Hand Shaking 과정 :
TCP의 연결을 해제(Connection Termination) 하는 과정

WPA 연구과정

WPA2-AES는 훨씬 뛰어난 보안성을 가지며, 이를 크랙하는 방법은 '무차별 대입 공격'이 유일하다. 4-Way Handshake 패킷을 캡처해 얻어 낸 5개의 매개변수 값과 사전 파일 안에 비밀번호 값을 이용해 Session Key를 생성한다. 공격자가 비밀번호로 예상되는 값으로 생성한 Session Key와 실제 Session Key를 비교한다. 따라서, 사전 파일 안에 비밀번호가 없다면 Crack에 실패하기 때문에 좋은 사전 파일을 가지고 있는 것이 중요하다.

1.사용자의 연결을 기다리거나, Dos공격을 통해 무선랜의 인증 절차를 유도해 4Way handshake 패킷을 수집한다.



2. 미리 준비해둔 사전파일 cracking-test와 4Way handshake 패킷이 담긴 파일을 비교해 비밀키를 찾아낸다.

결론

본 연구는 쉽게 간과하고 있는 무선 공유기 보안의 위험성에 대해 실험해본 후, 이를 통해 경각심을 갖고 개인 정보 보호의 필요성을 느낄 수 있고자 하는 목적으로 진행되었다. 실제로 Kali linux 프로그램을 이용하여 연구를 진행해본 바, 핸드폰과 와이파이 사이의 정보들을 볼 수 있었고 재전송 공격과 같은 공격도 가능하였다. 또한, 대문자, 소문자, 특수문자 등 다양한 문자를 섞어야 해킹 난이도가 높아진다는 사실도 알게 되었다. 이렇게 프로그램을 통하여 쉽게 해킹이 가능한 것으로 보아, 무선 공유기 해킹을 예방할 수 있는 방법을 아는 것이 더욱 중요해짐을 알 수 있다. 따라서 개인정보 보호를 위해서 단순하지 않은 적절한 비밀번호 설정과 공공 와이파이 암호화 등의 보안 강화가 필요하다. 본 연구를 통해 무선 공유기 해킹에 대해 경각심을 갖도록 하고 사람들이 개인 정보 보호에 힘쓸 수 있기를 기대한다.