WPA Based Packet Decrypt

POC 2015

발표에 앞서

- 이번 발표는 전혀 새로운 취약점을 발견해 낸 것은 아니며, WPA protocol 의 이해와 WPA packet 을 decrypt 할 수 있는 방법을 얘기하는 발표이다.

wireless packet analysis 에 대한 정보가 왜 적은가?

- wireless packet 을 잡을 수 있는 lan card 가 많이 보편화되어 있지 않기 때문이다.

monitor mode lan card 를 구하자

- 많은 사람들이 자신의 노트북이나 스마트폰에 무선 랜카드를 장착하고 있다. 하지만 대부분 이러한 랜카드는 monitor mode 를 지원하지 않는다.
- lan card 가 기본적으로 monitor mode 를 지원해야만 제대로 된 무선 packet 을 잡을 수 있다.

monitor mode 를 확인하는 방법

- monitor mode 지원 여부를 확인해 보도록 하자 .

wireless packet 을 잡아 보자

- 암호화 되어 있나?
  - 암호화되어 있는 조건은?
    - OPEN(???)
    - WEP(???)
  - 암호화되어 있지 않은 조건은?
    - WPA
    - WPA2
    - WPA2 Enterprise

How to decrypt wireless packet(open mode)

- (???) 영식이가 여기에 설명 추가 요망 (그림 , 자료 혹은 URL) 추가 요망 .

How to decrypt wireless packet(wep mode)

- (???) 영식이가 여기에 설명 추가 요망 (그림 , 자료 혹은 URL) 추가 요망 .

How to decrypt wireless packet(wpa mode)

- (???) 영식이가 여기에 설명 추가 요망 (그림 , 자료 혹은 URL) 추가 요망 .

How to decrypt wireless packet(wpa2 mode)

- (???) 영식이가 여기에 설명 추가 요망 (그림 , 자료 혹은 URL) 추가 요망 .

Demo

- 데모에 구현되어 있는 모듈은 크게 2 개로 구성되어 있다 .
  - wireless packet 을 잡아 일반 ethernet frame 으로 decrypt 하는 프로그램 (DeSniffer)
  - decrypt 된 ethernet frame 에서 cookie 를 추출하여 자신의 웹브라우저에 박아 놓는 프로그램 (cs)

Whrer can I download source code?

- open source 로 공개되어 있어요. 마음대로 공부하세요. :)
- https://github.com/wifihack

향후 계획

- 구현되어 있는 모듈들을 snoopspy 라는 project 로 통합 개발 .
- 향후 linux 환경뿐만 아니라 android, raspberry pi 및 arduino 로 porting 예정 .
- windows os 는 아몰랑 .

Any Question?

Q&A Time

Thank you

gilgil (http://gilgil.net)

yeongsik moon (http://bbolmin.tistory.com)