Project NAGA

:ARP Spoofing Detector

NAGA

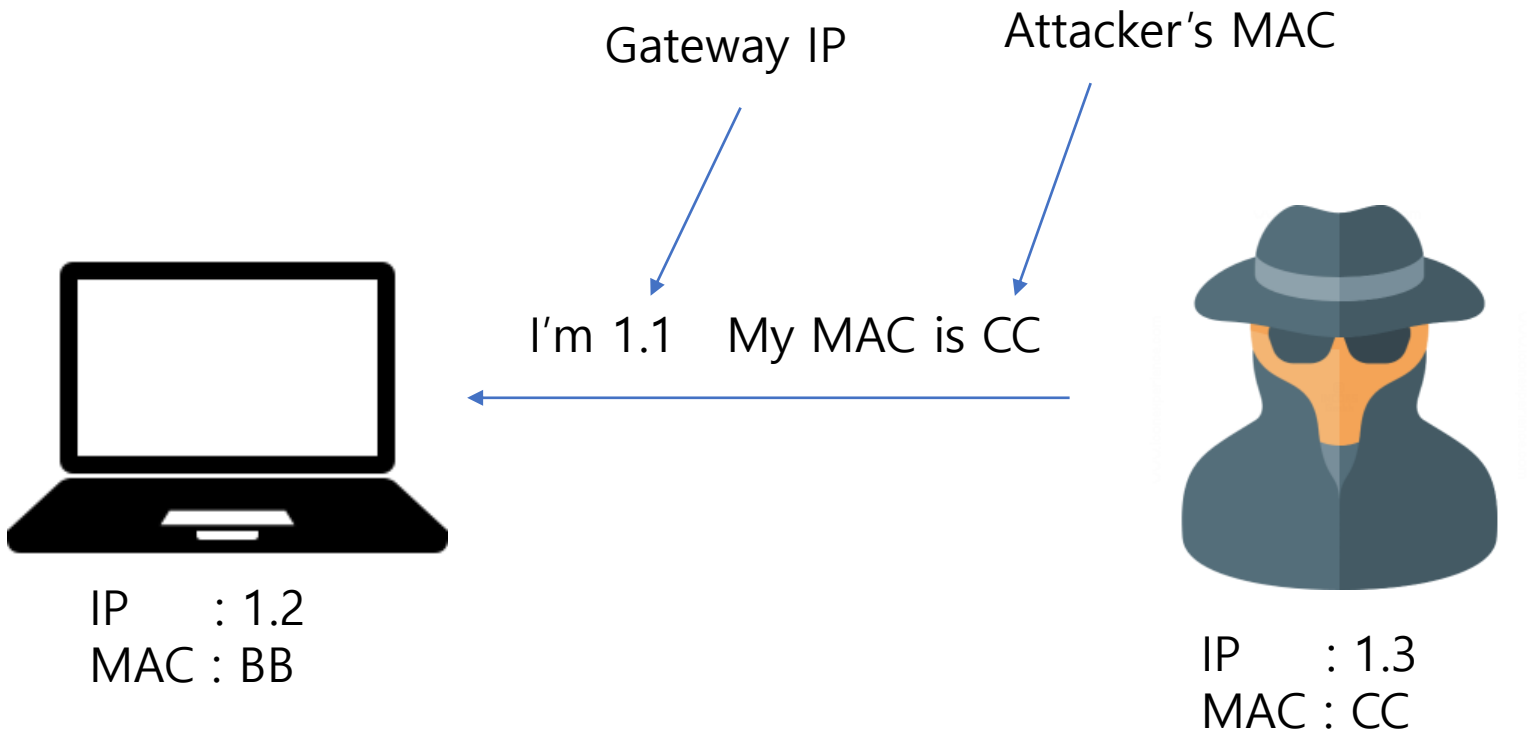
1. 초기 네트워크 연결시 Gateway의 맥 주소를 저장

2. ARP spoofing 공격 탐지....
 - Gateway의 맥주소 설정 변경을 요구 받으면 공격으로 판단

3. 공격자의 통신을 끊음
 - 공격자에게 게이트웨이가 사용할 수 없는 것 처럼 DoS 공격

4. Gateway와의 연결 복원
 - 원래의 내 맥주소를 Gateway에게 보냄

NAGA


Gateway IP
Attacker's MAC
I'm 1.1
My MAC is CC
IP : 1.2
MAC : BB
IP : 1.3
MAC : CC

NAGA

I'm 1.1 My MAC is CC

IP : 1.2
MAC : BB

IP : 1.3
MAC : CC

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

AA != CC

(3) Gateway와의 연결 복원!

I'm 1.2 My MAC is BB

IP : 1.2
MAC : BB

(1) Gateway의 맥주소 설정변경 요구

I'm 1.1 My MAC is CC

AP is not available
(Deauthentication Packet)

(2) 당신의 게이트웨이는 사용할 수 없는 상황입니다!

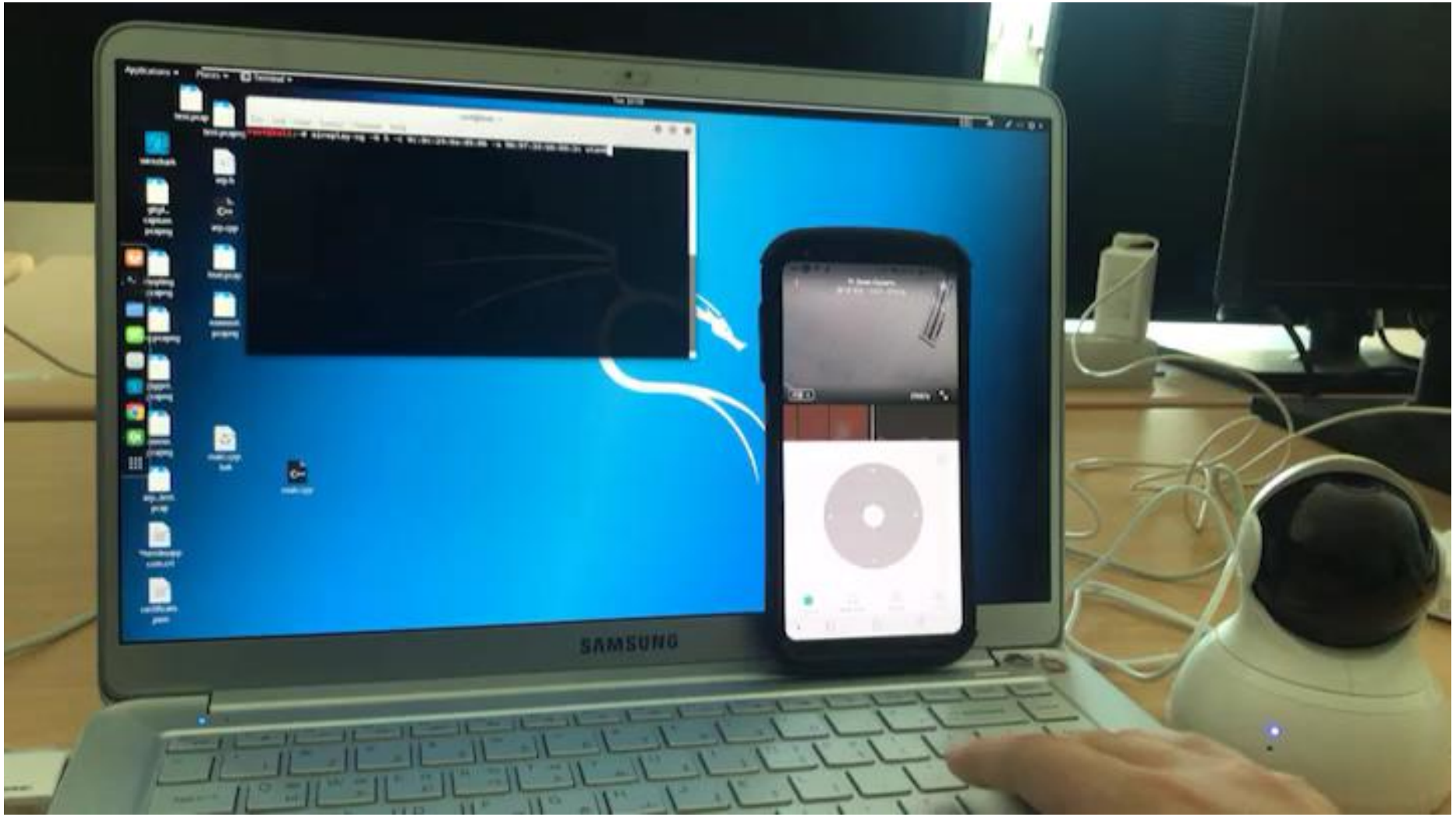
IP : 1.3
MAC : CC

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

AA != CC

Deautentication Packet 을 이용한 DoS 공격



문제점

1. 초기 네트워크 연결시 Gateway의 맥 주소를 저장
   → 애초에 ARP 스푸핑에 걸려있는 상태라면 Beacon frame을 이용해 맥주소를 parsing해야 함
   → Wireless 환경에서만 가능
2. ARP spoofing 공격 탐지....
 - Gateway의 맥주소 설정 변경을 요구 받으면 공격으로 판단
   → 그냥 단순히 Gateway가 바뀐 것이면 공격으로 판단하면 안됨...

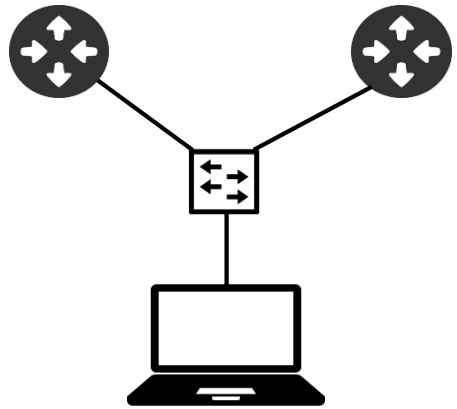
3. 공격자의 통신을 끊음
 - 공격자에게 게이트웨이가 사용할 수 없는 것 처럼 DoS 공격
   → DoS 공격을 보낼 때 네트워크 인터페이스를 사용 할 수 없음

4. Gateway와의 연결 복원
 - 원래의 내 맥주소를 Gateway에게 보냄

한계점

1. 그냥 MAC주소를 고정시키는 방법이 있지 않을까?
   -> 보통 arp스푸핑은 Wireless 환경에서 자주 일어나게 된다. 따라서 게이트웨이가 변하지 않는 환경이라면 고정시켜 놓는 것이 최선이다. 하지만 게이트웨이가 자주 변하는 Wireless 환경에서는 변할 때 마다 고정시켜 놓을 수 없기 때문에 (굉장히 귀찮기 때문에) NAGA가 꼭 필요하다.

2. 게이트웨이가 다중화 되어있을 때 게이트웨이 맥주소의 변화를 어떻게 arp 스푸핑과 다르게 탐지할 수 있을까?
   -> 두개 이상의 게이트웨이가 변화하면서 통신하는 환경이다. N개의 게이트웨이의 맥주소를 관리하는 방법밖에는...ㅠㅜ



발전방향

1. 로컬 네트워크의 경찰관 역할?
   (타인에 대한 공격을 탐지)

2. 누구나 사용할 수 있도록 tool 공개

3. 운영체제에 내장하는 방안