

IOT 프로젝트

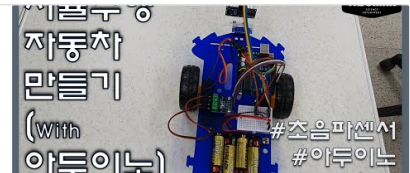
개요

- 아두이노를 활용한 IoT 기기 구현
- 구현한 기기 기반의 시나리오 기반 침투 실습(큰 주제는 아림님 아이디어 기반)
- 실습 후에는 보고서를 작성하여 해당 침투 취약점에 대한 분석 진행

IOT 기기 만들기

- 자율주행차 (초음파센서)

 <https://youtu.be/IuU7lsEYVig>



아두이노 자율주행자동차 만들기 1


아두이노 자율주행자동차 스케치로 아두이노 자율주행자동차 만드는 방법을 배워보겠습니다. 아두이노 자율주행자동차를 만들려면 모터, 서보모터, 초음파센서를 사용합니다. 초음파센서로 앞에 장애물이 있는지 확인하면서 앞으로 움직입니다. 그리고 장애물이 있으면 멈추고 서보모터를 움직여서 주위에 장애물이 있는지 확인하고, 움직이는 방향

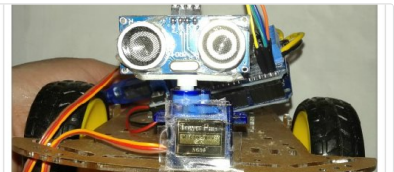
 <https://www.itple.co.kr/76>



아두이노 RC카 자율주행(장애물피하기) (아두이노) - Steemit

오늘은 몇일동안 포스트한 장애물을 피하는 자율주행 테스트 해보는 시간으로 내용을 채우고자 합니다. 좀 더 정교한 자율주행 코딩을 할까도 생각 했지만 처음은 단순한 장애물을 피하는 자율주행을 보여드리는 것이 좋을 것 같아서 종합 코딩은 간단하게 표현하여 자율주행의 의미를 전달하고자 합니다. 우선 초음파 아두이노 RC카를 사진으로만 보면

 <https://steemit.com/kr-arduino/@codingman/5nfqgd-rc>



- 헬스케어 기기
 - 심전도 측정 기기 (심박 펄스 센서)

26장. 아두이노 심박 펄스센서 사용하기!

안녕하세요. 인투피온입니다. 오늘은 심박 펄스 센서를 사용해서 심박수를 측정해 보도록 하겠습니다~ 요게...

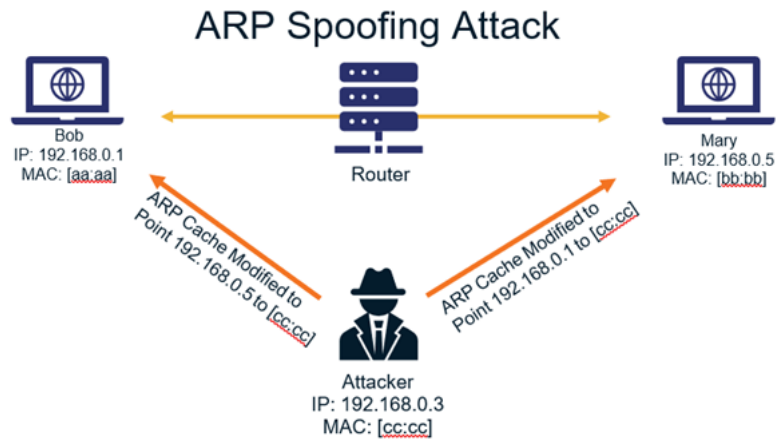
 <https://m.blog.naver.com/intopion/222009832752>



시나리오1

- 자율 주행 기능이 있는 IoT 기기 Alpha가 2차원 평면 f(20,60)에서 f(50,60)으로 이동하는 상황에서 외부의 공격자 K가 임의로 장애물이 존재하는 것처럼 보이도록 공격 수행, Alpha가 정지하도록 하는 시나리오

시나리오2



- 네트워크 취약점을 이용한 ARP 스푸핑 공격 실습
- 공격을 통한 패킷 위변조 or 접근 제어 우회(권한 상승)
- ARP Spoofing Attack : MAC 주소를 IP로 변환하는 프로토콜로서 통신하는 두 대상의 MAC 주소를 공격자 자신의 MAC 주소로 바꾸어 중간에서 패킷을 가로채는 공격
- 공격자가 bob에게 자신의 MAC주소를 mary의 MAC 주소인것처럼 속인다.
- 1. 공격자가 mary에게 자신의 MAC 주소를 bob의 MAC 주소인것처럼 속인다.
- 2. Bob는 mary의 MAC 주소가 CC(공격자)라 알고 있고, mary도 bob의 MAC 주소가 CC(공격자)라 알고 있다.
- 3. 공격자는 bob에게 받은 메시지를 mary에게 보내고, mary에게 받은 메시지를 bob에게 정상적으로 보내준다.
(이렇게 되면 정상적인 통신이 되며, 공격자는 메시지를 모두 읽을 수 있다.)
- 중간자 공격(Man in the Middle) : MITM 중간자 공격은 ARP 스푸핑에 의존하여 피해자 간의 트래픽을 가로채고 수정
- 희생자와 IoT기기 사이에서 공격자가 통신을 도청해서 패킷을 통해 민감 정보를 탈취하거나 패킷을 변조해 익스플로잇 (+수집된 패킷을 통한 권한상승공격)

시나리오3

- 악성코드 주입을 통한 봇넷 생성 및 DDoS 공격
- 포트 스캐닝으로 외부에 오픈되어 있는 포트를 찾은 후 포트에 악성코드를 주입해 봇넷 생성

ARP 스푸핑 공격 실습 예제

[https://blog.naver.com/PostView.naver?](https://blog.naver.com/PostView.naver?blogId=sunbei00&logNo=222264871331&parentCategoryNo=&categoryNo=49&viewDate=&isShowPopularPosts=true&from=search)

[blogId=sunbei00&logNo=222264871331&parentCategoryNo=&categoryNo=49&viewDate=&isShowPopularPosts=true&from=search](https://blog.naver.com/PostView.naver?blogId=sunbei00&logNo=222264871331&parentCategoryNo=&categoryNo=49&viewDate=&isShowPopularPosts=true&from=search)

<https://dundole.tistory.com/11>

실제로 민감정보가 노출되는 모습을 살펴보겠다.



[그림 13] 피해자의 로그인 패킷

위 패킷은 공격자의 PC를 통해 확인한 피해자가 로그인하기위해 보낸 HTTP요청이다. 피해자의 민감 정보가 그대로 노출된 것을 확인할 수 있다.

패킷조작 툴

BurpSuit : 서버와 클라이언트 사이 요청을 인터셉트 (중간에 프록시 서버를 만들어 패킷을 변조하여 내보낼 수 있음)

- <https://h-bread.tistory.com/15> // 사용방법
- <https://grini25.tistory.com/202> // 사용방법

프로젝트 진행 순서

1. 아두이노를 이용한 IOT 기기 제작
2. IOT 기기 취약점 분석
3. 시나리오 기반 IOT 익스플로잇
4. 패킷 분석을 통한 크리덴셜 탈취
 - a. 수집한 패킷을 변조하여 IOT 기기 익스플로잇
 - b. 수집한 패킷을 통한 권한 상승
5. 보고서 작성

#참고자료

https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

<https://southern-island.tistory.com/22>

<https://ddongwon.tistory.com/48>

<https://kkomii22.tistory.com/54>