

# Trip Report

ACM WiSec 2024

Koreana Hotel Gloria Hall (7th floor), Seoul, Korea  
May 27 - May 30, 2024

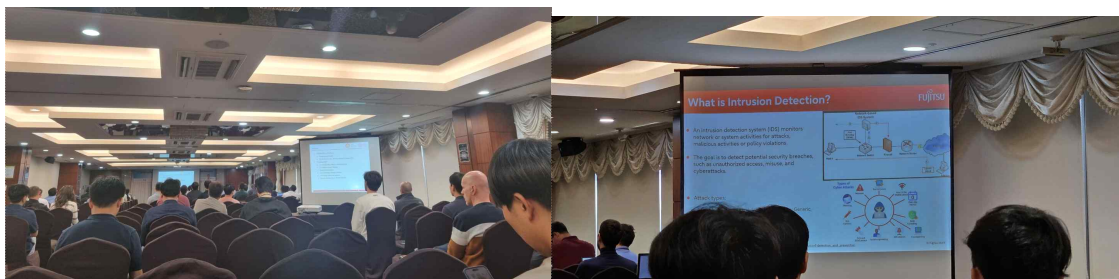
by GumJin Lee

## 개요

2024년 5월 무선 및 모바일 보안 학회인 ACM WiSec 2024가 서울 코리어나 호텔에서 개최되어 참석하였다. 이번 학회에는 5G/6G 이동통신 보안, ORAN 보안, 우주 보안, 무선 통신 보안, 사물인터넷 보안, 전기차 충전기 보안 등의 다양한 주제의 논문이 발표되었다. 분야가 기존에 하던 연구나 연구실 내의 다른 연구들과는 크게 달라서 다양한 분야의 연구들을 들어 보고 새로 배울 수 있는 기회가 되었다.



## WiSec 프로그램



9시부터 학회가 진행되었다. 9시부터 한시간 가량 Keynote 발표를 들 수 있었다. 이후 점심 전까지 세션 발표가 진행되었다. 세션 발표는 각 세션 별로 3~4개의 논문을 저자들이 발표하였다. 이후 점심식사 후에 짧게 Vision talk를 진행하고, 세션 발표가 두 번 더 있었다. 행사가 끝난 이후에는 포스터 발표나 연회 시간이 있었다. 이 중 인상 깊게 들었던 몇몇 발표를 소개하고자 한다.

### Watch Nearby! Privacy Analysis of the People Nearby Service of Telegram

People Nearby는 텔레그램이 제공하는 서비스로 사용자와 위치적으로 근접한 다른 사용자를 발견하는 서비스이다. 근처의 사용자들은 대략적인 위치로 나타나며 이를 통해 텔레그램은 위치 프라이버시를 지켰다고 주장한다. 저자는 사용자의 위치를 스푸핑하여 광범위한 측정을 시도했고, People Nearby가 사용자 간 거리를 계산하는 알고리즘을 역설계했다. 이를 기반으로 위치 프라이버시가 텔레그램이 주장하는 것보다 항상 낮다는 것을 입증했다.

측정 캠페인을 통해 데이터를 수집하였으며, 전 세계의 다양한 위치에서 총 302개의 측정을 통해 8,955개의 포인트를 수집했고 이 데이터를 기반으로 분석하여 위치를 추정하는 알고리즘을 개발하였다. 주요 결과로는 텔레그램이 주장하는 위치 프라이버시 반경은 500m인데 실제 결과는 항상 이보다 낮은 수준임을 확인했다. 특이한 점은 위도에 따라 달라지는데 사용자가 적도 근처에 있을 때는 400m, 극지방 근처에서는 128m까지 낮아졌다.

저자들은 이를 바탕으로 텔레그램의 People Nearby의 결함을 주장했으며, 위치 프라이버시를 보호하기 위해 여러 해결책과 대응 방안을 마련해야 한다고 주장했다. 그 예시로 저자들은 500m로 표시되고 있는 위치 정보를 불확실성 거리로 표현하거나, 높은 위도에서는 더 큰 타일을 사용하여 위치에 관계없이 500m의 영역을 나타내는 방법, API 정책을 변경하는 등의 해결방안을 제시한다.

이번 학기중의 공격자관점 보안 수업 중 다크웹과 딥웹에 관한 프로젝트를 진행하면서 텔레그램에 관한 언급을 많이 보았어서 텔레그램과 관련된 주제라서 집중해서 들었다. 텔레그램 자체의 약점보다는 서비스의 약점이라서 기대한 것과는 조금 달랐지만, 큰 규모의 연구를 위해 광범위한 데이터를 모으고 이를 분석하여 취약점을 찾아낸 점이 흥미로웠다.

## UWB-Auth: A UWB-based Two Factor Authentication Platform

이 논문에서는 휴대 가능하거나 착용 가능한 장치로 설계된 초광대역(UWB) 기반 이중 인증(2FA) 플랫폼인 UWB-Auth를 제안한다. UWB-Auth는 기존의 피싱, 2FA-fatigue, 동시 공격 등의 공격을 제거한다. 또한 사용자와 간단하고 빠른 상호작용을 제공한다.

기술의 핵심은 정밀 위치 인증으로, 스마트 워치, 스마트 링 등 인증 토큰이 로그인 장치와 가까운 곳에 있는지를 센티미터 단위의 정확도로 확인한다. 여기에 추가로 지식기반 또는 생체 인증 등을 추상화 계층으로 도입하여 사용자의 신원과 로그인 목적을 파악한다. 이 과정은 로그인 장치 근처의 토큰 유무를 확인하고 인증을 진행하므로, 전통적인 2FA의 검사 순서와 반대이며, 이는 데이터 유출에 대한 강력한 방어를 제공한다.

또한 저자는 UWB-Auth의 효과를 입증하기 위해 3가지 프로토타입을 제작하였다. 키체인 토큰, 상용 지식/생체 요소와 결합된 스마트워치, 맞춤형 지식/생체 요소와 결합된 스마트링을 제작하여 검증하였다. 전체적으로, UWB-Auth는 전체 인증과정을 4초 안에 완료하며, 물리적으로 허용되는 영역 밖에서 20cm 또는 10도 이상 떨어진 경우에 악의적인 접근을 완전히 차단한다. 심지어는 물리적으로 접근하더라도 지식/생체 인증을 통해 공격을 방어한다.

작년의 수업에서 2단계 인증에 관련된 프로젝트를 진행했었다. 당시에는 사용자 특성을 바탕으로 접근을 시도하는 사용자를 판별하여 2단계 인증을 생략하는 프로젝트였다. 다양한 정보를 수집했었지만 그 중에서 IP 주소를 통해 위치 정보도 획득했었는데, 지나치게 광범위하고 vpn을 통한 조작이 가능해서 실용적이지는 못하였다. 이 연구는 발전된 기술을 바탕으로 위치를 더 세밀하게 획득하고, 인증 과정까지 개선하여 더 효과적인 2단계 인증을 개발하여 인상 깊었다.

맺으며

사실상 첫 학회 참석 경험이었는데, 평소 보고 들던 분야와는 크게 다른 분야여서 어려운 내용도 많았고, 또 그만큼 흥미로운 내용도 많았다. 다양한 분야에 견문을 넓히는 것이 왜 필요한지 몸으로 깨닫게 되는 시간이었다.

아는만큼 보인다는 사실이 많이 체감되었다. 특히나 무선 통신이나 네트워크에 관한 분야가 중점이라 많은 발표들을 이해하는데 어려움이 있었다. 또한 행사가 진행되는 홀의 구조가 세로로 긴 구조라 뒤쪽의 참가자들은 발표를 듣는데도, 질문을 하는데도 어려움이 있었다. 좀 더 다양한 질문들이 나와서 들을 수 있었으면 좋았을 것 같다는 생각이 많이 들었다. 이와 별개로 영어 실력을 많이 늘려야겠다는 생각도 들었다. 실제 원어민들의 발표는 따라가는 것만으로도 벅했는데, 배경지식이 아닌 영어 실력으로 이해하지 못하는게 많이 부끄러웠다.

논문을 쓰는 것을 목표로 하고 좋은 학회에 논문을 내는 것을 목표로 하는 이상 언젠가는 나도 발표자의 역할로 학회에 참석하게 될 것이다. 그때 부끄럽지 않도록 더 열심히 준비하고 노력해야겠다.