Seminar Feedback Report (Week04)

2021312738 소프트웨어학과 김서환

4주차의 세미나 내용은 Mobile & Cloud Security 연구 분야에 대해 설명하는 내용이다. 주로 모바일과 클라우드 환경에서의 보안 취약점에 대한 내용이다. 안드로이드는 앱들 간의 활동 전환을 통한 상호작용 방식이 보안 취약점을 초래할 수 있다고 설명해주셨다. 공격자는 정상적인 앱의 활동과 유사한 화면을 만들어 사용자를 속이는 피싱 공격을 실행할 수 있다. 악성활동들이 목표 앱의 작업에 주입될 수 있기 때문에 작업에 대한 접근 제어가 부족하여 보안 취약점이 발생한다. 예를 들어, 페이스북 작업에 악성 활동이 주입되면 사용자가 페이스북 아이콘을 클릭할 때 악성 화면이 표시되어 공격을 할 수 있다고 설명해주셨다. 따라서 모바일 시스템에서 활동을 잘 보호하는 것이 중요한 보안 조치로 요구된다. 악성코드는 특별한 권한이나 복잡한 기술이 필요하지 않으며, launch mode, intent flag, task affinity에 따라 악성 활동이 작업에 주입될 수 있다. 더 자세하게는 안드로이드는 2가지의 launch mode, 7가지의 intent flag, 4가지의 callee launch mode가 있어서 이 조합으로 활동 주입에 대한 가능성이 많아진다고 설명해주셨다. 이러한 활동 주입을 탐지할 수 있는 도구에 대해 설명해주셨고, 실제 연구팀에서 정적 분석 도구를 통해 활동 주입 사례 1761개를 발견하였다고 설명해주셨다. 그리고 클라우드 보안에 관한 연구로 JNI(Java Native Interface)에 대해서 소개해주셨다. JNI는 java앱과 네이티브 코드간의 상호작용을 가능하게 하여 개발자들이 성능을 향상시킬 수 있도록 도와주는 인터페이스다. 하지만, JNI 함수(JNF)에 대한 잘못된 구현은 오류와 예외를 초래할 수 있으며 연구를 통한 검증이 필요하며, JustGen, OpenJ9 등의 JVM에서의 JNF 검증에 대한 얘기도 자세하게 해주셨다. 보안쪽은 평소에 잘 생각해보지 못했던 부분이라 왜 보안 취약점이 생기는지 구체적으로 어떤 부분에서 보안 취약점이 생기는지 알 수 없었지만 이번 4주차 세미나를 통해서 공격자가 어떤 방식으로 활동을 주입시키는지 원리에 대해 알 수 있어서 좋았다.