컴퓨터학콜로키움 **(COSE-405) :: 7**주차 우승훈 교수님

오픈소스 소프트웨어의 보안

강의 : 2022-10-19 / 작성 날짜 : 2022-10-19

고려대학교 컴퓨터학과 2017320108

고재영

인공지능, 기계학습과 같은 고도의 컴퓨터 관련 기술을 포함해서 현재 어느 궤도 이상으로 모든 분야에서 상당히 기술 발전이 이루어져 왔다. 기술 그 자체에게는 아니지만, 그 결과로는 많은 명과 암을 가져왔다. 이 중에 하나로 볼 수 있는 것은 해킹같은 보안과 관련한 문제를 꼽아 볼 수 있다. 날이 갈수록 악의적인 해킹, 크래킹과 악성코드의 수준은 발전에 발전을 거듭하고 있어 이에 대한 대비와 분석 대응의 중요성이 대두되고 있다. 이러한 보안에 대해서, 공격을 받은 이후 보안 취약점을 찾아 제거해나가는 사후 대응방식 뿐만 아니라 소프트웨어를 개발하는 단계에서 취약점을 찾아내고 미리 보완하여 대처하는 개발보안이 이에 해당한다고 볼 수 있다. 최근 행정안전부는 개발보안과 같은 시큐어코딩을 의무화하는 방향으로 정보보호에 관련하여 주의를 기울이는 노력을 보이고 있기도 하다. 보안에 관련한 코딩이 소프트웨어 개발자들에게 어느 정도 갖춰야할 소양으로 대두되는 오늘, 이 시간에는 우승훈 교수님께서 오픈소스 소프트웨어의 보안이라는 주제로 강연을 하셨다.

먼저 간단히 말해 오픈소스 소프트웨어는 대중에게 공개되어 있는 소프트웨어를 일컫는다. 완성되고 검증된 코드를 활용하여 다양하게 수정하여 사용할 수 있다는 점에서 시간적인 비용을 단축해주고 효율성을 증가시키는 소프트웨어 개발 환경에서 필수적인 점이라고 할 수 있다. 이러한 장점을 가지고 있지만, 불특정 다수의 사람이 접근가능한 만큼 오픈소스 소프트웨어에 있어서 보안의 중요성을 간과하는 것은 절대적으로 금물인데, 관리되지 않은 오픈소스 소프트웨어의 재사용은 여러 가지 보안 위협을 초래할 수 있기 때문이다. 해당 오픈소스에 대해 개발과정에서 미처 처리되지 못한 취약점들이 삽시간에 전파될 수도 있고, 라이선스를 위반하는 문제, 그리고 공급망이 공격당하는 데에 취약해지는 점 등이 이에 해당한다. 가령 최근 몇년동안 많은 사람들에게 화두가 되었던 암호화폐의 경우, 2018년

비트코인에서 이중지불의 문제를 야기하는 취약점이 발견되어 즉각적인 패치가 이루어졌지만, 비트코인 오픈소스의 코드를 재사용한 기반을 가진 일부 암호화폐는 즉각적으로 이에 대응하지 못해 막대한 금전 피해를 발생시켰다고 한다. 위와 같은 오픈소스 소프트웨어에 있어서 취약점을 탐지하기 위해 연사를 맡으신 우승훈 교수님이 주로 초점을 맞추신 방법은 소스코드 안에서의 취약점에 주목하는 정적 분석 기법을 집중하셨다고 한다. 이어서 설명하신 가장 간단한 하이레벨의 취약점 탐지 과정을 설명하셨는데, 취약점을 포함하고 있을 것으로 예상되는 오픈소스를 재사용한 타겟 프로그램의 소스코드를 분석하여, 취약코드가 전파되었는지 확인을 하는 방법이라고 한다. 기존에 있던 정적 분석에서는, 전파된 취약점에 대해 패치를 통해 삭제된 라인에 대해서만 고려하는 일차원적인 방식이었다. 이 경우 False Positives Error가 많이 발생하는 문제점을 야기하여 해당 라인뿐만 아니라 위아래 서너 라인을 추가로 확인하는 문맥을 고려하려는 노력을 시도했지만 실제 상황에서 위아래 문맥에선 공백이 주로 위치하였기 때문에 효과적이지 못했다. 또한 다른 방법으로 취약 코드가 포함되어 있는 함수 전체를 고려하는 방법도 시도되었지만, 이 경우 함수의 코드가 조금만 바뀌어도 취약점을 탐지하지 못하는 등 False Negative Error가 많이 발생하는 문제점이 있었다. 그래서 교수님께서 최근동안 진행하셨던 본인의 연구에서는, 너무 적은 패치 라인만을 고려하는 것은 아니면서, 함수 전체를 고려하는 것보단 스케일을 줄이면서 최적을 찾다보니, 취약점과 관련된 핵심 코드라인에 대해 control dependecy와 data dependency를 가지는 코드라인을 고려하는 방법을 찾으셨다고 했다. 그 결과로 False Positives / Negatives 각각에 대해서 오류 발생률도 효과적으로 줄이면서도 기존 기술에 대조적으로 6배 이상 더 많은 취약점 탐지에 성공적이었다고 한다.

학부 기간동안 보안에 관련한 강의를 안타깝게도 수강하지 못한 필자로서는 이번 강의는 매우 흥미로웠다. 연사 본인께서도 스타트업에 관련하여 종사를 하셨던 경험에서 말씀하셨지만, 단지 학부에서 어느 정도 코딩을 하는 과정에서 보안에 대해 약간 등한시했던 필자에게 보안이란 키워드를 생각해볼 수 있는 고무적인 기회였다. 마지막으로 가장 인상적이었던 점은 강연 마지막에 취약점 리포팅에 대한 해외 기업과 국내 기업들의 반응이었다. 취약점을 내부에서도 잡아내기 위해 많은 비용을 투자하는만큼 해외 기업들은 호의적인 반응이었던 반면에, 교수님의 경험으로는 국내기업들은 다소 껄끄러운 반응을 보였다는 점에서 아직 보안에 관련한 이슈로 취약점을 바라보는 인식의 차이가 상이하다는 점을 깨달았다.